Initiative 2025-2026 #270
Digital Property Rights and Restitution for Digital Harms

Received by Legislative Council Staff
3/6/26 at 5:21 AM

STATE OF COLORADO

AMPLIFY ACT — v28

RESIDENT DIGITAL AUTONOMY AND AUTOMATION MITIGATION ACT

A Bill for an Act Concerning Resident Digital Property Rights, Secure Enforcement Infrastructure, and the Creation of the Colorado Consumer Protection and Automation Mitigation Enterprise, Including Establishment of Resident Digital Soul Rights and a Master Deed Registry; the Colorado Trust of Unique and Identifying Information and the Office of Digital Oversight; Enterprise Mitigation Revenue Mechanisms; Programs-First Waterfall Distribution; UFIPA Trust Income Distribution to Residents; Thermal Recapture Infrastructure; Atmospheric Water Generation Credits; Water Replacement Mandates; Cascaded Dual-Cycle ORC Architecture; a Resident Mitigation Dividend; a Public Accountability Dashboard; and a Statutory Rate Schedule, and Making Appropriations Therefor.

AMPLIFY Act — Single Umbrella Bill | Title 15 Art. 15 · Title 10 Art. 10 · Title 24 Art. 20 | v28

ENACTING CLAUSE, SINGLE SUBJECT, AND CONSTRUCTION

Be it Enacted by the People of the State of Colorado:

Single subject. This act concerns the comprehensive governance of covered automation activity in Colorado — including the definition and protection of resident digital property rights arising from covered automation activity; the secure verification, enforcement, and accountability infrastructure required to administer those rights; the creation and administration of a government-owned business enterprise to assess and collect enterprise mitigation revenues and fund authorized mitigation measures; and the direct distribution of trust income and overflow revenues to Colorado residents — all necessarily and properly connected as components of a unified resident digital autonomy and automation mitigation framework. The three statutory articles established by this act operate as a single integrated system: resident property rights (title 15, article 15) are the source of the enterprise revenue base; the enforcement infrastructure (title 10, article 10) is the mechanism through which rights are verified and violations are detected; and the enterprise (title 24, article 20) is the mechanism through which revenue is collected, programs are funded, and residents receive direct distributions. No article operates independently of the other two — they are three legs of one structure.

Single-subject legal authority. Colorado courts apply the 'necessarily and properly connected' test under Article V, §21. All three articles of this act share a single unifying subject — the regulation of covered automation activity in Colorado for the protection and benefit of Colorado residents. The general assembly finds that: (a) the property right in §15-15-101 is the statutory predicate for the enterprise fee in §24-20-103 — no property right, no fee basis; (b) the enforcement infrastructure in title 10, article 10 is the operational mechanism without which neither the property right nor the enterprise revenue mechanism is administrable — no verification, no enforcement, no fee collection; and (c) the enterprise distribution in §§24-20-151 through 24-20-157 is the purpose for which the property right is

defined and the enforcement infrastructure is built. The three articles are not merely related — they are mutually dependent. Separating them is functionally impossible without destroying the operative effect of each.

Fee-for-service linkages. Any metered utility charge, token-output attribution charge, per-decision charge, valuation royalty, or reclamation fee in this act is a fee for the measurable service or externality identified in the fee's statutory predicate — not a tax. Each fee is proportional to the identifiable cost or externality it funds, as established by the cross-industry benchmark analysis in §24-20-156 and the fee-for-service linkage statement in §24-20-103. The fee-for-service linkage is uniform across all three articles of this act.

Construction — integrated operation. This act shall be construed as a single integrated statutory framework. No article shall be construed in isolation. Where a provision in title 15, article 15 cross-references the CCPAME, ODO, or Colorado Automation Mitigation Trust, that reference is operative regardless of which article establishes the referenced entity. Where a provision in title 10, article 10 cross-references resident rights established in title 15, article 15, that reference is operative without additional enacting language. The three articles are co-enacted, co-effective, and co-dependent.

Baseline administrative due process. Unless a more specific procedure is provided in this act, before imposing an adverse action against any covered entity, the CCPAME or ODO shall provide: (a) written notice of the alleged violation; (b) a reasonable opportunity to cure not less than thirty days for first violations; and (c) a written determination with findings. This baseline applies uniformly across all three articles.

SECTION 1. UNIFIED LEGISLATIVE DECLARATION

(1) Integrated findings. The general assembly finds and declares that: (a) The Digital Soul — encompassing biometric data, behavioral data, financial data, health data, location data, communications metadata, inferred identity attributes, and all other data uniquely identifying or profiling a Colorado resident — is inalienable intangible personal property of the resident from whom it is derived, and is the source of measurable economic value extracted by covered automation activity; (b) Covered automation activity generates measurable externalities — displacement of workers, erosion of resident data property rights, thermal waste, water consumption, and erosion of civic infrastructure funding capacity — that impose costs on Colorado residents, Colorado communities, and Colorado's shared resources; (c) A unified statutory framework — establishing resident property rights, secure enforcement infrastructure, and an enterprise mitigation revenue mechanism in a single act — is more effective, more resistant to evasion, and more administratively coherent than three separate acts that must interoperate through cross-references; (d) The property right, the enforcement mechanism, and the revenue enterprise are mutually dependent: the property right without enforcement is unenforceable; enforcement without a funded enterprise is unsustainable; and the enterprise without a property right predicate lacks constitutional fee-for-service grounding; (e) Thermal and water externalities of covered compute infrastructure are direct and quantifiable byproducts of covered automation activity and are properly mitigated through the enterprise established in this act; (f) Enterprise

mitigation revenues, held in the Colorado Automation Mitigation Trust and governed by UFIPA (C.R.S. §15-1.5-101 et seq.), generate Net Income Receipts that shall flow annually to registered Master Deed holders as the UFIPA Income Distribution, independent of and additive to the Resident Mitigation Dividend that flows from principal overflow after all program statutory reserve caps are fully funded; and (g) A statutory rate schedule benchmarked against comparable Colorado resource extraction and regulatory fee structures — held within Anti-Dilution Ratchet-protected floors and CCPAME-administered ceilings — ensures that enterprise fees are proportionate, fair across industries, and sufficient to fund the enterprise on a self-sustaining basis.

(2) Unified legislative intent. It is the intent of the general assembly that this act: (a) Define and protect The Digital Soul as inalienable intangible personal property of Colorado residents, enforceable through the Master Deed Registry, Audit Marker Signatures, and Synthetic Data Integrity Marker detection system; (b) Establish the Colorado Trust of Unique and Identifying Information and the Office of Digital Oversight as the secure enforcement infrastructure through which resident rights are verified, violations are detected, and covered operators are held accountable; (c) Create the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME) as a TABOR-exempt enterprise with independent revenues, independent governance, and a programs-first waterfall that funds child solvency, workforce transition, civic infrastructure, community stabilization, thermal recapture, and water replacement before distributing overflow to residents; (d) Generate two independent annual resident income streams — the UFIPA Income Distribution from Trust investment returns (flowing annually regardless of program cap status) and the Resident Mitigation Dividend from principal overflow (flowing when all eight program caps are fully funded) — both structured as property return distributions protected by the Anti-Dilution Ratchet and insulated from General Fund sweep; and (e) Operate as a self-funding, self-sustaining, permanently accountable enterprise whose financial status is visible to every Colorado resident in real time through the Mitigation Enterprise Public Accountability Dashboard.

ARTICLE STRUCTURE OF THIS ACT

PART I — RESIDENT DIGITAL PROPERTY RIGHTS (Sections 2–5): In Colorado Revised Statutes, add article 15 to title 15. Establishes The Digital Soul as inalienable intangible personal property; the Master Deed Registry; Audit Marker Signatures; Synthetic Data Integrity Marker Signatures; Decentralized Identity Verification Protocol consent framework; Resident Automated Mitigation Accounts; Base Dividend and Premium Royalty rights; Pre-Digital Operations Zones; Master Data Settlement and Restitution Agreement; and the MSSA disqualification framework.

PART II — SECURE ENFORCEMENT INFRASTRUCTURE (Sections 6–9): In Colorado Revised Statutes, add article 10 to title 10. Establishes the Colorado Trust of Unique and Identifying Information (air-gapped, FIPS 140-2 Level 3); the Office of Digital Oversight (ODO); Custodial Containment Protocols; Scheduled Compliance Verification Nodes; the

Non-Circumventable Incident Reporting System; Civic Enforcement Access Terminals; the Germaneness Mitigation Membrane; and secure facility safety standards.

PART III — AUTOMATION MITIGATION ENTERPRISE (Sections 10–13): In Colorado Revised Statutes, add article 20 to title 24. Establishes the CCPAME; Enterprise Mitigation Revenue mechanisms; the Colorado Automation Mitigation Trust; programs-first waterfall (§§24-20-151–152); Resident Mitigation Dividend (§24-20-153); Investment Reserve (§24-20-154); Public Accountability Dashboard (§24-20-155); Statutory Rate Schedule (§24-20-156); UFIPA Income Distribution (§24-20-157); Thermal Recapture Infrastructure (§§24-20-140–148); Agricultural AWG Credits (§24-20-149); Water Replacement Mandate (§24-20-150); and Cascaded Dual-Cycle ORC Architecture (§24-20-143(7)–(10)).

FEDERAL PREEMPTION SAVINGS CLAUSE — UMBRELLA ACT. This act shall operate to the maximum extent permitted by federal law. If any provision of any part of this act is found to be federally preempted, that provision is severable; the remaining provisions and the remaining parts of the act continue in full force and effect. Each of the three statutory articles established by this act is independently severable from the other two — federal preemption of any provision of title 10, article 10 does not affect the operative provisions of title 15, article 15 or title 24, article 20, except to the extent the preempted provision was the sole predicate for a cross-referenced obligation, in which case the CCPAME and ODO shall administer an equivalent protection by rule pending legislative remedy.

APPROPRIATION NOTE — UMBRELLA ACT. No General Fund appropriation is required for ongoing operations. The three statutory articles established by this act are funded exclusively through enterprise mitigation revenues collected from covered operators. Startup costs across all three articles are authorized as a single contingency General Fund loan, repayable from first-year revenues within eighteen months of the CCPAME's first revenue collection event. The UFIPA Income Distribution and Resident Mitigation Dividend are distributions of trust income and overflow — not state fiscal year spending for TABOR purposes.

— PART I BEGINS ON NEXT PAGE — RESIDENT DIGITAL PROPERTY RIGHTS (Title 15, Article 15) —

PART I — RESIDENT DIGITAL PROPERTY RIGHTS

Title 15, Article 15 — Sections 2 through 5 of this act

— END PART I | PART II BEGINS ON NEXT PAGE — SECURE ENFORCEMENT INFRASTRUCTURE (Title 10, Article 10) —

PART II — SECURE ENFORCEMENT INFRASTRUCTURE

Title 10, Article 10 — Sections 6 through 9 of this act

— END PART II | PART III BEGINS ON NEXT PAGE — AUTOMATION MITIGATION ENTERPRISE (Title 24, Article 20) —

PART III — AUTOMATION MITIGATION ENTERPRISE

Title 24, Article 20 — Sections 10 through 13 of this act

SECTION 2. In Colorado Revised Statutes, add article 15 to title 15 as follows:

ARTICLE 15 — PERSONAL DATA AND DIGITAL PROPERTY RIGHTS

15-15-101. ***Definitions.***

As used in this article 15, unless the context otherwise requires:

(1) "The personal data and derived inferences" means the totality of a resident's digital identity and emergent automation-generated property, including: (a) biometric data — any data derived from a resident's physical or physiological characteristics, including fingerprints, retinal scans, facial geometry, voiceprints, gait patterns, DNA sequences, and physiological signals; (b) behavioral data — any data derived from a resident's habits, routines, preferences, patterns of movement, purchasing decisions, communication patterns, or other behavioral attributes; (c) derived biological data — any inference, prediction, score, profile, or classification derived from biometric or behavioral data, including health risk scores, emotional state assessments, neurological inferences, and fertility or vulnerability indicators; (d) civic telemetry — location data, transit data, voting and civic participation data, government service interaction records, and infrastructure usage data; and (e) all emergent automation-generated inferences derived from any of the foregoing. The personal data and derived inferences is the inalienable intangible personal property of the resident from whom it derives. No covered entity may assert ownership, perpetual license, or lien against The personal data and derived inferences.

(2) "Master Deed" means the official digital property rights record establishing a resident's ownership of their personal data and derived inferences, registered with the state, cryptographically anchored in the Colorado Trust of Unique and Identifying Information, and accessible by the resident through the myColorado platform or Civic Access Infrastructure.

(3) "Audit Marker Signature" means a uniquely-tagged, synthetically generated data artifact embedded within a resident's personal data and derived inferences profile — invisible in ordinary use — that serves as an irrefutable, cryptographically verifiable evidence marker of unauthorized ingestion, scraping, or training, triggering automatic statutory damages upon detection.

(4) "Resident Automated Mitigation Account" means the resident-controlled account within the Colorado Automation Mitigation Trust established under article 20 of title 24 that receives Premium Royalty payments triggered by Tier 2 Data Tap events under section 15-15-110.

ROYALTY FLOOR. ***Minimum per-person annual royalty; CPI-indexed.***
(1) Minimum annual royalty. Where this article requires or authorizes payment of a royalty, dividend, or compensation amount to a resident for authorized use of the resident’s protected data, inferences, or derived works, the payment schedule shall include a minimum annual royalty floor per eligible resident.
(2) Floor amount. The minimum annual royalty floor is two hundred fifty dollars ($250) per eligible resident per covered operator, per calendar year, unless a higher floor is established by rule. The floor is adjusted annually for inflation under the inflation adjustment section of this article.

(3) Pro-rata and de minimis. The administrator may adopt rules to pro-rate the floor for partial-year eligibility and to prevent duplicative payment where multiple controlled affiliates are treated as a single operator, but shall not set a de minimis threshold that defeats the floor.

(5) "Master Data Settlement and Restitution Agreement" or "Legacy Use Settlement Agreement" means an enforceable agreement entered between the attorney general and a historical violator under section 15-15-130, resolving claims arising from unauthorized Digital Soul extraction, training, scraping, or monetization occurring prior to the effective date of this article.

(6) "Legacy Use Settlement Program" means the Legacy Use Settlement Agreement enforcement strategy authorized under section 15-15-130 by which the attorney general leverages the combined weight of statutory damages triggered by Audit Markers, enterprise assessments under article 20 of title 24, and existing AG enforcement powers to compel historical violators into comprehensive settlements.

(7) "Digital Deed" means the enforceable legal title instrument embedded within a resident's Master Deed that specifies the resident's consent grants, restrictions, royalty entitlements, and Generative Veto rights with respect to specific categories of the resident's personal data and derived inferences.

(8) "Generative Veto" means a resident's right to prohibit any covered entity from using the resident's personal data and derived inferences to generate, train, fine-tune, augment, or produce any synthetic output, model output, or downstream commercial product.

(9) "Mandatory Disconnection" means a resident's right to demand that a covered entity permanently delete, purge, and certifiably destroy all copies of the resident's personal data and derived inferences data, including training corpora, model weights, and embeddings, within the timeframes established by rule.

(10) "Analog " means a designated physical space in which a resident has activated the Non-Networked Isolation Protocol, exercising their right to an analog environment free from automated sensing, capture, or automated-mediated interaction.

(11) "Compute Parity" means a resident's right to access the same quality, capability, and feature tier of covered automation services available to commercial customers of the covered entity, without algorithmic downgrade, throttling, or capability restriction based on the resident's personal data and derived inferences consent profile or exercise of rights under this article.

(12) "Civic Access Infrastructure" means the physical access infrastructure established under section 15-15-140, including myColorado ID kiosks at county centers, that enables residents without digital access to exercise all rights under this article, including Master Deed registration, transactions, consent updates, and loading of Resident Automated Mitigation Account benefits cards or linked bank accounts.

(13) "Joint Household Veto Power" means the consent right established under section 15-15-141 by which a lawfully married spouse or registered domestic partner may co-sign or veto consent grants, royalty disbursements, or Resident Automated Mitigation Account transactions on behalf of the household, subject to individual resident primacy and anti-coercion safeguards.

(14) "Restoration Credits" means non-cash mitigation credits issued by the CCPAME for the limited purpose of defraying measurable externalities arising from Emergent

Automation, redeemable only through direct-to-provider payment rails or other fiduciary spend-control protocols. Restoration Credits are not cash and may not be withdrawn as cash.

(15) "Covered entity" means any person or business entity that deploys, operates, offers, sells, licenses, leases, or provides a covered emergent automation system in Colorado, or that commercially delivers such a system to or targets Colorado residents.

(16) "Intake Firewall" means the technical and contractual control system through which a covered entity verifies consent before ingesting, processing, or training on Digital Soul data.

(17) "Decentralized Identity Verification Protocol" means a cryptographically verifiable, resident-issued consent signal anchored to the resident's Master Deed, constituting valid consent for a specific, scoped use of Digital Soul data.

THE DIGITAL SOUL AS INALIENABLE PROPERTY — MASTER DEED

15-15-102. The Digital Soul — Inalienable Intangible Personal Property — No Waiver — No Conversion.

(1) Inalienability. The Digital Soul is the inalienable intangible personal property of the resident from whom it derives. A resident's ownership of their Digital Soul: (a) cannot be waived, assigned, forfeited, or surrendered by any contract, terms-of-service agreement, or consent form, except through the limited, revocable, scoped consent mechanisms established in this article; (b) cannot be levied upon, liened, garnished, or taken in satisfaction of any debt or obligation of the resident except as authorized by court order under procedures established by rule; (c) survives the resident's death and passes to their designated heir or estate as intangible personal property.

(2) No perpetual license. Any contract term, terms-of-service clause, license grant, or data-processing agreement purporting to convey a perpetual, irrevocable, or royalty-free license to a resident's Digital Soul is void ab initio as against public policy.

(3) Consent revocability. Any consent granted by a resident for use of Digital Soul data is revocable at will, subject to reasonable technical wind-down periods established by rule, not to exceed ninety (90) days.

15-15-103. ***Master Deed Registry — Registration — Digital Deed Instrument — Cryptographic Anchoring.***

(1) Establishment. The secretary of state, in coordination with the ODO established under title 10, article 10, shall establish and maintain the Master Deed Registry as the official state record of resident digital property rights.

(2) Registration. Any Colorado resident may register a Master Deed, at no cost, through: (a) the myColorado digital platform; or (b) an Civic Access Terminal at any county service center, subject to section 15-15-140.

(3) Digital Deed instrument. A Master Deed shall include one or more Digital Deed instruments specifying: (a) the categories of Digital Soul data the resident authorizes for use; (b) the specific purposes, time limits, and royalty rates applicable to each authorization; (c) any Generative Veto, Mandatory Disconnection demands, or Analog designations; and (d) the resident's Resident Automated Mitigation Account routing information for Premium Royalty payments.

(4) Cryptographic anchoring. Each registered Master Deed shall be cryptographically anchored as a Resident Identity Verification Hash in the Colorado Trust of Unique and Identifying Information established under title 10, article 10, creating an immutable, verifiable record of the resident's digital property rights.

(5) Interoperability. The secretary of state shall establish a standard API enabling covered entities to query Master Deed consent status for Digital Soul data categories, subject to privacy-preserving, zero-knowledge verification methods that do not expose the resident's full Master Deed to the querying entity.

SYNTHETIC DATA INTEGRITY MARKER SIGNATURES — STATUTORY DAMAGES TRIGGER

15-15-104. Audit Markers — Unauthorized Ingestion Detection — Statutory Damages.

(1) Authority and purpose. The ODO shall develop and maintain a library of Audit Markers — uniquely-tagged synthetic data artifacts — that may be registered by residents within their Master Deed profiles for the purpose of detecting unauthorized ingestion, scraping, or training by covered entities.

(2) Activation and embedding. A resident may, through their Master Deed registration or Civic Access Infrastructure, activate one or more Audit Markers to be embedded within their Digital Soul profile. The resident shall not be required to disclose the specific nature or location of embedded Audit Markers to any covered entity.

(3) Detection and automatic trigger. When the ODO detects that a Audit Marker Signature has appeared in a covered entity's model outputs, training data, or inference pipeline — demonstrating unauthorized ingestion — the detection event shall: (a) constitute conclusive, irrefutable evidence of unauthorized use of the associated resident's Digital Soul without a valid Decentralized Identity Verification Protocol; (b) automatically trigger statutory damages under subsection (4); and (c) constitute a predicate act for the Legacy Use Settlement Agreement Legacy Use Settlement Program under section 15-15-130.

(4) Statutory damages. Upon confirmed Audit Marker detection, the affected resident shall be entitled to statutory damages of not less than: (a) five thousand dollars ($5,000) per detected unauthorized use; (b) ten thousand dollars ($10,000) per detected Audit Marker where the unauthorized use involved generation of a synthetic likeness of the resident; (c) twenty-five thousand dollars ($25,000) per detected Audit Marker where the unauthorized use involved the resident's

biometric or derived biological data. Statutory damages accrue per violation and are cumulative. They do not require proof of actual damages.

(5) AG referral and class aggregation. The ODO shall transmit Audit Marker detection events to the attorney general for enforcement. The attorney general may aggregate individual Audit Marker detection events across residents into a class enforcement action or as predicates for an Legacy Use Settlement Agreement proceeding under section 15-15-130.

(6) Covered entity liability. A covered entity that has ingested a Audit Marker Signature is strictly liable for the statutory damages in subsection (4). It is not a defense that the ingestion was automated, inadvertent, or conducted by a contractor or processing partner.

MASTER SETTLEMENT AND SOVEREIGNTY AGREEMENT — ROPE-A-DOPE

15-15-130. Master Settlement and Master Data Settlement and Restitution Agreement — Legacy Use Settlement Agreement — Legacy Use Settlement Program Enforcement Strategy — Historical Violator Compulsion.

(1) Purpose and authority. The attorney general is authorized and directed to pursue Master Settlement and Master Data Settlement and Restitution Agreements with covered entities that have engaged in historical violations — the unauthorized extraction, scraping, ingestion, training upon, or commercial monetization of Colorado resident Digital Soul data prior to or after the effective date of this article. The Legacy Use Settlement Agreement mechanism, known as the Legacy Use Settlement Program, leverages the combined weight of: (a) Audit Marker statutory damages under section 15-15-104; (b) enterprise assessments and Digital Severance Assessments under article 20 of title 24; (c) existing attorney general enforcement powers under the Colorado Consumer Protection Act and the Colorado Privacy Act; and (d) reputational and market-access consequences of non-settlement to compel comprehensive remediation agreements.

(2) Legacy Use Settlement Agreement components. An Legacy Use Settlement Agreement negotiated under this section shall include, at minimum: (a) a full accounting and disclosure of all Colorado resident Digital Soul data ingested, trained upon, or monetized; (b) retroactive royalty payments calculated using the Digital Severance Assessment rates in section 24-20-116, applied to all historical severance events; (c) a forward-going compliance plan, including Intake Firewall deployment, Decentralized Identity Verification Protocol integration, and Master Deed API compliance; (d) a resident restitution fund, administered through the Colorado Automation Mitigation Trust under article 20 of title 24, for distribution to affected residents whose Audit Markers were detected or who can demonstrate unauthorized use of their Digital Soul; and (e) enhanced monitoring and reporting obligations for a period of not less than five (5) years.

(3) Legacy Use Settlement Program sequencing. The attorney general shall implement the Legacy Use Settlement Agreement Legacy Use Settlement Program

in the following sequence: (a) Phase 1: Audit Marker activation — the ODO activates and embeds Audit Markers across the resident population, beginning to accumulate irrefutable evidence of unauthorized use by covered entities; (b) Phase 2: Assessment notices — the CCPAME issues Digital Severance Assessment notices and enterprise fee obligations to historical violators, creating an escalating financial pressure; (c) Phase 3: Legacy Use Settlement Agreement demand — the attorney general transmits Legacy Use Settlement Agreement demand letters to identified historical violators, presenting the aggregated Audit Marker evidence and financial exposure; (d) Phase 4: Negotiation — the attorney general conducts settlement negotiations, with the understanding that failure to settle results in full statutory damages, treble damages for willful conduct, and public enforcement action; (e) Phase 5: Settlement or litigation — the attorney general executes an Legacy Use Settlement Agreement or initiates formal litigation.

(4) No statute of limitations waiver required. The Legacy Use Settlement Agreement mechanism operates prospectively from the effective date of this article. The attorney general's existing legal authority governs any claims regarding conduct prior to the effective date, and this section does not constitute a limitation or waiver of any such authority.

(5) Public Legacy Use Settlement Agreement registry. The attorney general shall maintain a public registry of executed Legacy Use Settlement Agreements, including the identity of the settling entity, the scope of the agreement, the total restitution fund established, and the compliance monitoring obligations, subject to redaction of protected trade secrets and individual resident information.

DATA TAP FINANCIAL ROUTING — TIER 1 AND TIER 2

15-15-110. Data Tap Financial Routing — Tier 1 Base Dividend — Tier 2 Premium Royalty — Resident Automated Mitigation Account.

(1) Purpose. Enterprise Mitigation Revenue mechanism is the financial routing mechanism that connects resident Digital Soul property rights to the Enterprise Mitigation revenue system under article 20 of title 24, ensuring that every commercial use of Digital Soul data generates a resident financial benefit.

(2) Tier 1 — Anonymous data — Base Dividend. When a covered entity uses Digital Soul data that has been verified as anonymized or de-identified, consistent with objective standards established by rule, the Colorado Trust of Unique and Identifying Information shall generate a Tier 1 Data Tap signal. The Tier 1 signal triggers a Base Dividend calculation, with proceeds flowing into the Colorado Automation Mitigation Trust under article 20 of title 24 for distribution as part of the Enterprise Mitigation Revenue, including child solvency funds, mental health interventions, housing stabilization, and analog bridge infrastructure.

(3) Tier 2 — Identifying data — Premium Royalty. When a covered entity uses Digital Soul data that contains personally identifying information, distinct persona links, or Digital Soul attributes that can identify or re-identify a resident, the Colorado Trust of Unique and Identifying Information shall generate a Tier 2 Data

Tap signal. The Tier 2 signal triggers a Premium Royalty calculation. Premium Royalty proceeds shall be routed directly to the individual resident's Resident Automated Mitigation Account via the Colorado Trust. Premium Royalty payments are the resident's private property and may be disbursed as cash, loaded onto a linked benefits card or bank account, or applied to Restoration Credits at the resident's election.

(4) Rate schedule. The CCPAME shall establish, by rule, the Base Dividend and Premium Royalty rate schedule, calibrated to the Digital Severance Assessment rates in section 24-20-116. The rate schedule shall ensure that Tier 2 Premium Royalty rates are materially higher than Tier 1 Base Dividend rates, creating a persistent financial incentive for covered entities to obtain full Decentralized Identity Verification Protocol consent rather than relying on de-identification.

(5) Resident access to Resident Automated Mitigation Account. A resident may access their Resident Automated Mitigation Account through the myColorado platform or any Civic Access Terminal, including for cash disbursement, card loading, bank account transfer, or allocation to child solvency or household mitigation funds.

CIVIC ACCESS INFRASTRUCTURES AND myColorado ID — SPOUSAL VETO POWER

15-15-140. Civic Access Infrastructures — Physical Kiosk Infrastructure — myColorado ID — Universal Access.

(1) Establishment. The state shall establish and maintain a statewide network of Civic Access Infrastructure access points, located at county service centers, public libraries, and other accessible public facilities, ensuring that every resident — regardless of digital access, technical literacy, or disability status — can exercise all rights under this article in person, through a human-staffed process or a myColorado ID kiosk.

(2) Required Civic Access Infrastructure functions. Every Civic Access Infrastructure access point shall enable a resident to: (a) register, update, or revoke a Master Deed and Digital Deed instruments; (b) submit Mandatory Disconnection demands; (c) activate or deactivate Audit Markers; (d) access their Resident Automated Mitigation Account balance, transaction history, and disbursement options; (e) load Resident Automated Mitigation Account funds onto a linked benefits card or linked bank account; (f) file complaints, submit grievances, and access ODO intake services; and (g) request Legacy Use Settlement Agreement-related restitution fund applications.

(3) myColorado ID integration. The myColorado ID platform shall serve as the digital-physical bridge interface, enabling residents to: (a) authenticate through a physical government-issued ID without requiring a smartphone or internet connection; (b) receive a printed receipt of all transactions and registrations for personal records; and (c) access a human navigator who can assist with complex transactions or special circumstances.

(4) Parity requirement. Civic Access Infrastructure services shall be substantively equivalent in scope, timeliness, and quality to digital platform services. No right under this article may be conditioned on digital access. The state shall ensure that processing times for Civic Access Infrastructure transactions do not materially exceed digital transaction processing times.

(5) Funding. The costs of establishing and maintaining Civic Access Infrastructure infrastructure shall be funded from the Analog Access Implementation Fund established under title 10, article 10, consistent with the fee allocation tables in section 10-10-160.

15-15-141. Joint Household Veto Power — Household Co-Consent and Transaction Co-Authorization.

(1) Purpose. The general assembly finds that Digital Soul rights and Resident Automated Mitigation Account assets are household assets with shared family implications. A resident who is lawfully married or in a registered domestic partnership may designate their spouse or partner to exercise limited co-consent and co-authorization rights over Digital Soul transactions, providing an additional layer of household protection without overriding individual resident primacy.

(2) Scope of Joint Household Veto Power. A resident's designated spouse or domestic partner may, upon written designation by the resident: (a) co-sign or veto consent grants for Digital Soul data uses above a transaction threshold established by rule; (b) co-authorize Resident Automated Mitigation Account disbursements above a household disbursement threshold established by rule; and (c) receive joint notification of Audit Marker detection events and Legacy Use Settlement Agreement restitution fund eligibility determinations affecting the household.

(3) Individual resident primacy. The Joint Household Veto Power does not override individual resident control. A resident may at any time revoke the Joint Household Veto designation unilaterally. A resident's individual consent grant or revocation remains valid notwithstanding the absence of spousal co-signature, except within the transaction thresholds established pursuant to subsection (2).

(4) Anti-coercion safeguards. The secretary of state and the ODO shall establish rules to prevent coercive use of the Joint Household Veto Power, including: (a) automatic suspension of Joint Household Veto authority upon the filing of a protection order, domestic violence allegation, or court order addressing coercion; (b) a resident's right to terminate the Joint Household Veto designation through any Civic Access Infrastructure without spousal co-authorization; and (c) training for Civic Access Infrastructure navigators on recognizing coercion indicators.

(5) Civic Access Infrastructure registration. A Joint Household Veto Power designation may be made, modified, or revoked through the myColorado platform or any Civic Access Terminal, without requiring digital access or attorney assistance.

DIGITAL SOUL RIGHTS — CORE CONSUMER PROTECTIONS

15-15-105. Intake Firewall — Decentralized Identity Verification Protocol — Consent Architecture.

(1) No covered entity may ingest, process, train on, or commercially monetize any category of Colorado resident Digital Soul data without a valid, cryptographically verifiable Decentralized Identity Verification Protocol anchored to the resident's Master Deed.

(2) Any data ingested without a valid Decentralized Identity Verification Protocol is Contraband Data, subject to the enforcement provisions of title 10, article 10, and the statutory damages provisions of section 15-15-104.

(3) Consent scope. A Decentralized Identity Verification Protocol is valid only for the specific data categories, purposes, time periods, and compensation terms specified in the resident's Digital Deed. Any use beyond the scoped consent is an unauthorized use triggering statutory damages.

15-15-106. *Generative Veto — Mandatory Disconnection — Right to Destruction.*

(1) Generative Veto. A resident may at any time invoke a Generative Veto through their Master Deed, prohibiting any covered entity from using the resident's Digital Soul to generate, train, fine-tune, augment, or produce any synthetic output, model output, or downstream commercial product.

(2) Mandatory Disconnection. A resident may demand Mandatory Disconnection, requiring a covered entity to permanently delete, purge, and certifiably destroy all copies of the resident's Digital Soul data, including training corpora, model weights, and embeddings, within ninety (90) days of the demand, or a shorter period established by rule.

(3) Certification. A covered entity that receives a Mandatory Disconnection demand shall provide a cryptographically verifiable certification of destruction, filed with the ODO, within the applicable destruction period.

15-15-107. Post-Mortem Data Disposition Directive — Authorized Successor Data Designation — Pre-Digital Property Archive.

(1) Post-Mortem Data Disposition Directive. A resident may include in their Master Deed a Post-Mortem Data Disposition Directive requiring all covered entities holding the resident's Digital Soul data to execute Mandatory Disconnection within ninety (90) days of confirmed notification of the resident's death.

(2) Authorized Successor Data Designation. A resident may designate a Authorized Successor Data Designation — a protected archive of specified Digital Soul data categories — to be preserved, transferred to a designated heir, or maintained in mitigation custodial custody by the Colorado Trust of Unique and Identifying Information following the resident's death.

(3) Pre-Digital Property Archive. Where a resident does not execute a Post-Mortem Data Disposition Directive or Authorized Successor Data Designation designation, covered entities holding the resident's Digital Soul data shall apply default privacy

protections established by rule, preventing commercial use without authorization from the designated heir or estate.

15-15-108. ***NCII Prohibition — Nonconsensual Intimate Imagery — Emergency Injunctive Relief.***

(1) Prohibition. No covered entity may generate, distribute, host, transmit, or commercially benefit from nonconsensual intimate imagery (NCII) involving a Colorado resident, including automated-generated or synthetic NCII.

(2) Strict liability. NCII violations are strict-liability offenses. The existence of NCII attributable to a resident in a covered entity's systems or outputs, without verifiable consent, constitutes the violation.

(3) Emergency injunctive relief. A resident who is a victim of NCII may seek emergency injunctive relief in any court of competent jurisdiction, including an ex parte temporary restraining order requiring immediate takedown, without bond, upon a credible showing of the violation.

(4) Damages. In addition to injunctive relief, a resident who prevails on an NCII claim shall be entitled to: (a) actual damages; (b) statutory damages of not less than twenty-five thousand dollars ($25,000) per violation; and (c) attorney's fees and costs.

15-15-109. ***Minor Protections — Guardianship Credentialing — Dual-Consent Protections.***

(1) No covered entity may ingest, process, or use the Digital Soul data of a minor without the verified, informed consent of the minor's parent or lawful guardian, in addition to the minor's affirmative assent where age-appropriate.

(2) Legacy tracking technologies default-off. All tracking, profiling, and data-retention features for minor residents shall default to off and may be activated only through dual consent — the guardian and the minor (age 13 and over) — with clear, plain-language notice.

(3) Guardian credentialing. A parent or guardian exercising consent rights over a minor's Digital Soul must credential through the Master Deed registry, establishing a guardianship link that is auditable by the ODO and terminates automatically upon the minor reaching majority.

CONSTITUTIONAL AMENDMENT DIRECTIVE

15-15-150. Constitutional Amendment Directive — General Assembly Referral — Digital Soul as Inalienable Property Under the Colorado Constitution.

(1) Findings. The general assembly finds that the rights established in this article — the ownership of The Digital Soul as inalienable intangible personal property — are so fundamental to resident sovereignty, economic participation, and

protection from emergent automation harms that they require constitutional protection against future legislative erosion.

(2) Directive to the General Assembly. The general assembly is hereby directed, not later than the first general session following the effective date of this act, to: (a) draft a proposed constitutional amendment to the Colorado Constitution that enshrines The Digital Soul — including biometric data, behavioral data, derived biological data, and civic telemetry — as inalienable intangible personal property of every Colorado resident; (b) include in the proposed amendment the protections of the Master Deed, the Generative Veto, and the right to Mandatory Disconnection as fundamental resident rights that no future legislative act may abrogate without voter approval; and (c) refer the proposed constitutional amendment to the voters of Colorado at the next general election occurring at least ninety (90) days after the date of referral.

(3) Proposed amendment scope. The proposed constitutional amendment shall, at minimum: (a) define The Digital Soul as the biometric, behavioral, derived biological, and civic telemetry data of a resident, along with all emergent automation-generated inferences derived therefrom; (b) declare The Digital Soul to be the inalienable intangible personal property of the resident, co-equal in dignity and legal protection with tangible personal property; (c) prohibit any law, contract, terms-of-service agreement, or government act that purports to permanently alienate, waive, or extinguish a resident's Digital Soul rights without just compensation and voter approval; and (d) guarantee the Symbiotic Sovereignty principle — that a resident's digital existence and physical existence are inseparable, and that the rights of one cannot be severed from the other without the resident's free, informed, and revocable consent.

(4) Savings; statutory rights preserved pending amendment. The rights established in this article are enforceable as statutory rights pending voter approval of any constitutional amendment and shall not be diminished or suspended pending the referendum.

(5) Ballot language. The general assembly shall cause the proposed constitutional amendment to be placed on the ballot with language approved by the title board that clearly and accurately describes to voters: (a) the meaning of The Digital Soul as personal property; (b) the nature of the Symbiotic Sovereignty principle; and (c) the specific rights and protections to be constitutionalized.

OPTION B — PHASED SCALE-UP — CAPABILITY PARITY

15-15-114. ***Phased Compliance — Option B Scale-Up — Privacy Minimization — Payment Rail Privacy.***

(1) General. Covered entities shall come into compliance with this article according to the phased schedule and option pathways established by rule, provided that all entities shall be in full compliance not later than three (3) years after the effective date of this act.

(2) Option B — phased scale-up with privacy minimization. A covered entity that elects Option B compliance shall implement the Intake Firewall and Decentralized Identity Verification Protocol architecture on a phased schedule established by rule, provided that: (a) the entity demonstrates a good-faith compliance roadmap within ninety (90) days of the effective date; (b) privacy minimization is implemented in each phase, reducing unauthorized ingestion progressively; and (c) full compliance is achieved within the deadline established in subsection (1).

(3) Payment rail privacy by design. Any payment processing or compensation infrastructure used to route Premium Royalty or Base Dividend payments to residents shall be designed with privacy-by-default, ensuring that payment transactions cannot be used to profile, track, or re-identify residents.

(4) Capability parity. No covered entity shall algorithmically downgrade, throttle, or deny Compute Parity to a resident based on the resident's exercise of Digital Soul rights, consent profile, or Generative Veto. Violation of this section constitutes a deceptive trade practice under the Colorado Consumer Protection Act.

INFLATION ADJUSTMENT. ***Inflation adjustment for fixed-dollar amounts.***
(1) Any fixed-dollar amount, threshold, cap, minimum, maximum, penalty, statutory damages amount, or fixed-dollar rate set forth in this article shall be adjusted annually on January 1 by the administrator to reflect inflation. The adjustment must be based on the Consumer Price Index for All Urban Consumers (CPI-U), U.S. City Average, as published by the Bureau of Labor Statistics, or a successor index. The base year is the first full calendar year in which this article is operative.
(2) The administrator shall publish the adjusted amounts no later than December 1 of each year for the following calendar year, rounded to the nearest whole dollar. This section does not apply to amounts expressed as a percentage, a market-indexed benchmark, or a formula that automatically adjusts with price level.

SECTION 3. SEVERABILITY

If any provision of this act or its application is found invalid, such invalidity does not affect other provisions that can be given effect without the invalid provision. The provisions of this act are declared severable.

SECTION 4. SAFETY CLAUSE

The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

additions: Digital Soul property definition | Legacy Use Settlement Agreement Legacy Use Settlement Program | Audit Markers | Data Tap Tier 1/2 | Civic Access Infrastructure | Joint Household Veto Power | Constitutional Amendment Directive

CONSTRUCTION; SCOPE OF COMMERCIAL PROCESSING.
(1) For purposes of this act, “commercial processing” includes collection, scraping, ingestion, training, fine-tuning, evaluation, storage, labeling, or other use of resident Digital Soul data when conducted by or for a covered operator in connection with a product, service, system, or capability that is offered, licensed, used, or deployed in commerce, whether or not the specific processing step is described as research, development, testing, or internal evaluation.
(2) A covered operator shall not evade the consent and Master Deed authorization requirements by characterizing a monetizable data ingestion or training pipeline as noncommercial research.

IMPLEMENTATION SCHEDULE — TIERED PHASE DEPLOYMENT

15-15-900. Implementation schedule.

(1) Immediate rights and protections.
The following provisions take effect immediately upon enactment of this act:

(a) Recognition of the Digital Soul as resident-owned intangible personal property.
(b) Enforceability of Master Deed authorization and consent controls.
(c) Prohibition on unauthorized extraction or commercial processing of the Digital Soul.
(d) Establishment of the Colorado Trust of Unique and Identifying Information.
(e) Authorization of the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME).
(f) Authorization of the Colorado Automation Mitigation Trust.
(g) Authority for responsible agencies to promulgate rules necessary to implement this act.

These provisions constitute self-executing statutory rights and are not dependent upon technical system deployment.

(2) Phase I — Administrative establishment (0–12 months).
Responsible agencies shall establish:

(a) the Colorado Trust of Unique and Identifying Information;
(b) the Colorado Automation Mitigation Trust;
(c) enterprise accounting mechanisms for the Enterprise Mitigation Revenue;
(d) rulemaking for Master Deed authorization standards, inter-system monitoring standards, and enterprise compliance reporting.

(3) Phase II — Compliance infrastructure (12–24 months).
Covered operators shall implement:

(a) tamper-evident metering systems;
(b) inter-system safety monitoring controls;
(c) incident detection telemetry;
(d) Digital Soul consent verification mechanisms.

During this phase the following revenue mechanisms activate:
High-Density Compute Grid Surcharge, Autonomous Kinetic Asset Registration, Silicon-to-Carbon Reclamation Assessment, and the Algorithmic Risk Pool.

(4) Phase III — Public mitigation programs (24–36 months).
The state shall deploy:

(a) staggered civic infrastructure loans at 1%, 2%, and 3% APR;
(b) mitigation programs funding child solvency, housing stabilization, and healthcare or mental-health services.

Interest collected through civic infrastructure loans shall be swept into mitigation accounts within the Colorado Automation Mitigation Trust.

(5) Phase IV — Long-term stability and oversight (36 months onward).

The following provisions become fully operational:

(a) the Statutory Revenue Floor and dynamic rate adjustments;
(b) workforce displacement transition and vocational reskilling programs;
(c) full enterprise audit cycles and public reporting requirements.

15-15-140. Data Tap; tiered routing; Base Dividend; Premium Royalty.
(1) Tier 1 — anonymous routing. Tier 1 extraction of the Digital Soul that is processed only in anonymous or aggregated form shall remit a Base Dividend to the Colorado Automation Mitigation Trust pursuant to title 24, article 20.
(2) Tier 2 — identifying routing. Tier 2 extraction of the Digital Soul that includes identifying processing shall remit a Premium Royalty routed to the resident's Resident Automated Mitigation Account through the Colorado Trust of Unique and Identifying Information, subject to Master Deed authorization.
(3) Mathematical routing requirement. Covered operators shall implement accounting controls that separately meter Tier 1 and Tier 2 processing volumes and shall remit payments under this section according to rules adopted pursuant to title 24, article 20. Tier 2 processing is prohibited absent Master Deed authorization.

15-15-160. Heritage assets; analog-era vehicles; mechanical sanctuary.
(1) Definitions. For purposes of this section:
(a) “Heritage asset” means an analog-era vehicle that is maintained for personal use and that satisfies the physical barrier requirements of subsection (2) of this section.
(b) “Physical barrier” means a verifiable mechanical override that physically disconnects all external telemetry pathways and disables externally addressable automated kinetic control interfaces, such that remote connectivity cannot be restored without physical intervention.
(2) Certification. The administering agency shall establish a certification process to verify that a vehicle meets the physical barrier requirements necessary to qualify as a pre-digital mechanical asset.
(3) Privacy shield; prohibited mandates. For a certified pre-digital mechanical asset, a state agency, political subdivision, or state contractor shall not require:
(a) continuous connectivity;
(b) installation of externally addressable telemetry modules; or
(c) over-the-air updates as a condition of registration, inspection, insurance eligibility, or operation within the state.
(4) Construction. This section does not limit lawful safety recalls that can be accomplished without removing or defeating a certified physical barrier.

15-15-170. Joint Household veto power for shared family interfaces.
(1) Applicability. If a covered operator offers a shared family interface that permits access to, control of, or authorization over Digital Soul processing for more than one resident within a household, the covered operator shall provide a mechanism for spousal veto as described in this section.
(2) Veto authority. A spouse or civil union partner with shared-interface authority may revoke or withhold authorization for Tier 2 identifying Data Tap routing and for any shared-interface permissions that enable identifying processing of that spouse’s Digital Soul, notwithstanding conflicting interface settings initiated by another household user.
(3) Verification and logging. The covered operator shall verify the identity of the vetoing party using Master Deed authorization controls and shall record the veto event in an immutable authorization log.
(4) Construction. Nothing in this section authorizes a spouse to consent to identifying processing of another resident’s Digital Soul without that resident’s Master Deed authorization.

INDEPENDENT OPERABILITY; COORDINATION; SEVERABILITY.
(1) Independent operability. This act is intended to be independently operable and enforceable. No duty, authority, remedy, assessment, program, or right created by this act is conditioned on the enactment, adoption, or effectiveness of any other measure.
(2) Coordination. If another measure concerning the Digital Soul, the Colorado Automation Mitigation Trust or Enterprise Mitigation Revenue, the Colorado Trust of Unique and Identifying Information, or any related public utility or enterprise framework is enacted, the responsible agencies may coordinate implementation to avoid duplication; however, coordination is permissive and does not limit or delay enforcement of this act.
(3) Harmonization of definitions. If another enacted measure defines terms also used in this act, the definitions shall be construed harmoniously to the greatest extent possible. If an irreconcilable conflict exists, the definition in this act controls for purposes of this act.
(4) Severability. If any provision of this act or its application is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application.
(5) Rights are immediate. The recognition of the Digital Soul as inalienable intangible personal property and the Master Deed authorization requirements are self-executing and apply immediately upon enactment, regardless of whether any enterprise, trust, or utility program is established by any other measure.

ANNEX — DEFINITIONS ALIGNMENT AND CONTROLLING TERMS

The following definitions govern any conflict between this act and companion documents. The definition in this act controls in all cases.
Controlling term: 'The Digital Soul' (§15-15-101(1)) is the operative statutory term throughout. References in companion documents to 'resident digital identity information' or 'personal data' shall be construed to mean The Digital Soul as defined herein.
Controlling term: 'Master Data Settlement and Restitution Agreement' (Legacy Use Settlement Agreement) supersedes any prior reference to 'Master Settlement and Master Data Settlement and Restitution Agreement' in all companion documents.
Controlling term: 'Pre-Digital Operations Zone' supersedes the truncated 'Analog' reference in §15-15-101(10) of prior drafts.
Controlling term: 'Colorado Automation Mitigation Trust' (§24-20-104, title 24, article 20) supersedes any prior designation for this trust' in all companion documents.
Controlling term: 'UFIPA Income Distribution' (§24-20-157) means the annual distribution of Net Income Receipts from Colorado Automation Mitigation Trust investment holdings to registered Master Deed holders, independent of and additive to the Resident Mitigation Dividend. Residents receive both distributions annually from their Resident Automated Mitigation Account.
Controlling term: 'Statutory Rate Schedule' (§24-20-156) means the binding rate schedule with floors, initial rates, and ceilings for all Enterprise Mitigation fees. CCPAME may only move rates within the statutory band. Harmonization rule: In the event of any irreconcilable conflict between a definition in this act and a definition in any companion document, fiscal impact statement, or administrative record, the definition in this act controls for purposes of this act.

FEDERAL PREEMPTION SAVINGS CLAUSE

Federal preemption. This act shall operate to the maximum extent permitted by federal law. If any provision of this act is found to be preempted by federal law, that provision is severable pursuant to the severability clause of this act, and the remaining provisions continue in full force and effect. Nothing in this act shall be construed to conflict with the Supremacy Clause of the United States Constitution; rather, this act is expressly designed to operate within Colorado's reserved powers under the Tenth Amendment to regulate intrastate commercial activity, protect Colorado residents' property rights, and impose fees for measurable externalities caused by covered automation activity within Colorado. To the extent any provision may be construed to conflict with federal law, the CCPAME shall interpret and administer this act in a manner that avoids such conflict while preserving the maximum scope of resident protection authorized under state law.

APPROPRIATION NOTE

No General Fund appropriation required. This act does not require an appropriation from the Colorado General Fund. The Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME) is a government-owned business enterprise funded entirely by enterprise mitigation revenues collected from covered operators under this act. Startup administrative costs incurred prior to initial enterprise mitigation revenue collections are authorized as a contingency loan from the General Fund, to be repaid from first-year enterprise mitigation revenues within eighteen (18) months of the CCPAME's first revenue collection event. This loan authorization does not constitute a continuing appropriation.

SECTION 2. In Colorado Revised Statutes, add article 10 to title 10 as follows:

ARTICLE 10 — SECURE INFRASTRUCTURE AND JUSTICE

10-10-101. ***Definitions.***

As used in this article 10, unless the context otherwise requires:

(1) "Air-gapped" means physically isolated from the public internet and from any external network such that no data can be transmitted to or from the system except through controlled, logged, and authenticated transfer procedures.

(2) "Non-Networked Isolation Protocol" means a mandatory hardware-level circuit-break and physical disconnection capability for covered Emergent Automation systems, providing resident-controlled, local physical disconnection of automated sensing, capture, actuation, and networked automation functions, with enhanced requirements in designated sanctuary and pre-digital mechanical assets.

(3) "The Colorado Trust of Unique and Identifying Information" or "The Trust" means the proprietary, decentralized, and air-gapped state storage and audit environment established under this article, operating as the state verification and audit infrastructure — the primary sovereign repository and funding trigger mechanism for the Enterprise Mitigation Revenue established under article 20 of title 24. The Trust is designed to support zero-knowledge audit proofs, contraband-data compliance verification, and secure Digital Soul mitigation custodial services. The Trust operates strictly as a blind fiduciary repository. It is structurally prohibited from continuous data ingestion and may only house cryptographic Resident Identity Verification Hashes and human-triggered Static Incident Artifacts pending verification by the Panel.

(4) "state verification and audit infrastructure" means the function of the Colorado Trust of Unique and Identifying Information as the primary cryptographic verification and triggering mechanism for Enterprise Mitigation revenue events, including the Data Tap routing that distinguishes Tier 1 (anonymous) data events from Tier 2 (identifying) data events for purposes of Base Dividend and Premium Royalty calculations under article 20 of title 24.

(5) "The Panel" means a paid, human-in-the-loop workforce of temporary civic workers tasked with verifying algorithmic flags and compliance events under the two-step verification process.

(6) "Contraband Data" means any data ingested, processed, stored, trained upon, or used without a valid, cryptographically verifiable Decentralized Identity Verification Protocol or in violation of an Intake Firewall.

(7) "Colorado Automation Mitigation Custodial Account" means state-held encrypted custody of Digital Soul or resident audit artifacts in a fiduciary capacity, utilizing cryptographic access controls and key management to prevent unauthorized access and to require judicially authorized procedures for unmasking.

(8) "Judicial Cryptographic Token" or "JCT" means a time-bound, rotating session token serving as the lock-and-key mechanism authorized by a Triad Review Panel for the limited purpose of unmasking or accessing protected audit data.

(9) "Shadow Person Output" means an anonymized tokenized audit artifact that omits facial and direct identifiers, used for initial verification by the Panel to preserve privacy.

(10) "Triad Review Panel" means a mandatory oversight body consisting of a prosecutor, a defense attorney, and a magistrate serving as the authorization authority for high-level data access, unmasking, and intensive audits.

(11) "Two-step verification" means the process by which two independent, randomized verifiers confirm an alleged contraband-data event or compliance violation before any adverse action may issue.

(12) "CSAM" means any visual depiction of sexually explicit conduct involving a minor, as defined by applicable state and federal law.

(13) "Synthetic CSAM" means any computer-generated or emergent automation-generated depiction that depicts a minor engaging in sexually explicit conduct, regardless of whether it is derived from an identifiable real minor.

(14) "Zero-Tolerance Compute Mandate" means the strict-liability operational requirement that prohibits any covered entity from using compute resources to generate, transform, distribute, store, train on, or otherwise process CSAM or Synthetic CSAM.

(15) "Covered entity" or "covered operator" means any person or business entity that deploys, operates, offers, sells, licenses, leases, or provides a covered emergent automation system in Colorado, or that commercially delivers such a system to or targets Colorado residents.

(16) "Facility Chain-of-Command Incident Reporting System" means the verifiable, non-circumventable chain-of-command incident reporting, verification, and escalation system for detention facilities established under section 10-10-150.

(17) "Civic Enforcement Access Terminal" or "Jail Kiosk" means the secure, tamper-evident inmate-facing terminal deployed under section 10-10-151 for resident reporting, grievance intake, legal access, and Non-Circumventable Incident Reporting incident submissions.

(18) "Master Log" means the immutable, tamper-evident, continuously maintained record of all Non-Circumventable Incident Reporting incident submissions, verification actions, escalation decisions, and warden determinations required under section 10-10-152.

(19) "Three-Strike Escalation" means the mandatory review and escalation protocol under section 10-10-153 by which an unresolved or disputed Non-Circumventable Incident Reporting report progresses through three independent review levels culminating in final warden determination.

(20) "Resident Identity Verification Hash" means a cryptographic one-way hash of a resident's Digital Soul identifiers stored within the Colorado Trust of Unique and Identifying Information, used for zero-knowledge verification without exposing underlying resident data.

(21) Delegated system; operator responsibility. Any model, automated system, tool, contractor, processor, or service operating under the authority, license, or delegation of a covered entity is deemed an extension of that covered entity for purposes of duties, enforcement, and liability under this article.

(22) "Verified Incident Record" or "VIR" means a verifiable, non-destructive incident record created only after two-step verification, consisting of the underlying source record references, the Shadow Person Output or other minimized artifact reviewed, the identities (or authenticated

reviewer IDs) of both independent verifiers, timestamps, the verification outcome (sustained, not sustained, or inconclusive), and any escalation or unmasking authorization issued under this article.
(23) "Adverse action" means any action that materially affects a person's liberty, legal status, access to goods or services, employment, housing, credit, benefits, education, medical care, custody status, detention conditions, account access, or that initiates, escalates, or materially influences a referral to law enforcement, issuance of a citation, trespass order, detention, or similar enforcement consequence.
(24) "Authorized Successor Data Designation" means an encrypted, resident-governed, append-only record container within or interoperable with the Trust, designed to preserve a durable record for a household or family group, subject to multi-party authorization for critical actions, non-destructive corrections, and continuity/portability requirements under section 10-10-108.6.

THE COLORADO TRUST OF UNIQUE AND IDENTIFYING INFORMATION — state verification and audit infrastructure

10-10-103. The Colorado Trust of Unique and Identifying Information — Sovereign Air-Gapped Storage — state verification and audit infrastructure — Zero-Knowledge Audits.

(1) The state shall establish and maintain the Colorado Trust of Unique and Identifying Information as an air-gapped, decentralized storage and audit environment, operating as the state verification and audit infrastructure — the sovereign origin point and primary verification mechanism for all Enterprise Mitigation revenue events authorized under article 20 of title 24.

(2) The Trust shall: (a) support receipt and verification of zero-knowledge audit proofs for contraband-data compliance without requiring public disclosure of proprietary source code, model weights, or trade secrets; (b) maintain immutable audit logs for all access attempts and all JCT authorizations; (c) serve as the cryptographic trigger mechanism for Data Tap financial routing events, distinguishing Tier 1 anonymous data events from Tier 2 identifying data events for purposes of Base Dividend and Premium Royalty calculations; (d) provide resident-facing access through the myColorado platform for Resident Identity Verification Hash registration, certificates, notices, and audit attestations, as authorized by law.

(3) Data Tap Financial Routing — state verification and audit infrastructure trigger function. The Trust shall implement the Data Tap as follows: (a) Tier 1 Data Events. When the Trust verifies a covered data transaction involving anonymized or de-identified data as defined by rule, the Trust shall generate a Tier 1 Data Tap signal. The Tier 1 signal triggers a Base Dividend calculation into the Colorado Automation Mitigation Trust under article 20 of title 24. Tier 1 events carry the lower assessment rate established under section 24-20-116(2)(b). (b) Tier 2 Data Events. When the Trust verifies a covered data transaction involving personally identifying information, distinct persona links, or Digital Soul attributes that can identify or re-identify a resident, the Trust shall generate a Tier 2 Data Tap signal. The Tier 2 signal triggers a Premium Royalty calculation routed directly to the resident's Resident Automated Mitigation Account via the Trust. Tier 2 events carry the higher assessment rate established under section 24-20-116(2)(a).

(4) The ODO shall establish certification standards for entities that integrate with the Trust, including secure transfer procedures, logging, and key management.

(5) No continuous ingestion. The Trust is structurally prohibited from continuous data ingestion. It may only house Resident Identity Verification Hashes and human-triggered Static Incident Artifacts pending verification by the Panel.

10-10-104. Colorado Automation Mitigation Custodial Account — Fourth Amendment Protection Architecture.

(1) The state may hold encrypted Digital Soul and resident audit artifacts in Colorado Automation Mitigation Custodial Account.

(2) Mitigation custodial custody under this section: (a) does not transfer title or beneficial ownership of resident property to the state; (b) requires adherence to strict fiduciary duties, including confidentiality, minimization, and purpose limitation; (c) is designed to reduce third-party seizure risk and to require judicially supervised procedures for access.

(3) No state employee shall access protected data held in mitigation custodial accounts except pursuant to a valid Judicial Cryptographic Token issued under section 10-10-105, and only to the minimum extent necessary for the authorized purpose.

TRIAD REVIEW PANEL AND JUDICIAL CRYPTOGRAPHIC TOKEN

10-10-105. ***Triad Review Panel — Judicial Cryptographic Token — Due Process.***

(1) The Triad Review Panel is hereby established. The chief judge of each judicial district shall designate magistrates to serve, and the ODO shall maintain rosters of qualified prosecutors and defense attorneys.

(2) A Judicial Cryptographic Token may issue only upon: (a) a sworn application stating the specific scope of data access sought, the factual basis for the request, and the minimization procedures to be employed; (b) a finding by the Triad Review Panel that the request is narrowly tailored and supported by probable cause or other applicable legal standard; (c) a determination that less intrusive means are unavailable or insufficient.

(3) Each JCT shall: (a) be time-limited and scope-limited; (b) permit only the minimum unmasking or access necessary for the authorized purpose; (c) generate immutable logs within the Trust.

(4) The ODO shall implement standardized notice procedures, including delayed notice where authorized by court order.

(5) Community Supervision — Court-Ordered Condition; Limited Whereabouts Access. Notwithstanding the JCT requirements of this section, limited, real-time access to a resident's whereabouts data by the Department of Corrections or the Judicial Department is authorized only when such access is an express condition of supervision imposed by a court, parole authority, or other lawful supervising authority. Tiered

authorization: (I) Standard supervision requires concurrent digital authorization of both the assigned supervising officer and the officer's direct supervisor. (II) Intensive supervision requires the digital authorization of the assigned supervising officer. Access shall be limited to the minimum data necessary and shall not include bulk historical location history beyond a narrowly tailored time window. Any whereabouts data unmasked shall automatically generate an immutable audit log within the Trust.

(Y) Emergency guardian tether for minors — active missing-child alert. When a minor resident is the subject of an active, verified Colorado Bureau of Investigation AMBER Alert or Endangered Missing Alert, a custodial parent or lawful guardian may authorize an emergency decryption tether for the limited purpose of locating the minor. The tether shall automatically expire at the earliest of: (I) cancellation of the alert; (II) confirmation the minor has been recovered; or (III) twenty-four (24) hours after activation, unless renewed pursuant to an active alert. Any data unmasked shall generate an immutable audit log within the Trust.

(Z) Voluntary kinship tether for adults — life-safety activation; no state key custody. Two adult residents may, by mutual consent, establish a voluntary kinship tether through a peer-to-peer authorization method. The State and The Trust shall not hold persistent decryption keys for voluntary kinship tethers. A request to activate may be honored only during a verifiable life-safety emergency corroborated by independent objective signals. Any activation request shall immediately trigger an unblockable, device-level notification to the targeted resident, who retains an always-on veto. Default disablement applies where there is an active civil protection order between the parties.

EYE IN THE SKY — CHAIN-OF-COMMAND REPORTING SYSTEM

10-10-150. Non-Circumventable Incident Reporting System — Purpose — Architecture — Non-Circumventability.

(1) Purpose. The general assembly finds that detention facilities present acute, demonstrable civil-liability and public-safety risks arising from unreported misconduct, retaliatory silencing of residents, and inadequate chain-of-command accountability. The Non-Circumventable Incident Reporting System is hereby established as a verifiable, non-circumventable digital chain-of-command for sensitive conduct reporting within detention facilities, ensuring that every incident report is verified, logged, escalated appropriately, and resolved with documented finality.

(2) Architecture. The Non-Circumventable Incident Reporting System shall: (a) receive incident reports submitted by residents through the Civic Enforcement Access Terminal under section 10-10-151 or by staff through authenticated duty-status terminals; (b) automatically verify submission integrity using cryptographic time-stamps, tamper-evident hashing, and kiosk session logs stored in the Colorado Trust of Unique and Identifying Information; (c) route verified reports to the appropriate level of the facility chain of command based on the category and subject of the report as established in subsection (3); (d) automatically escalate any report that implicates a supervisor, official, or staff member to that person's direct superior within the chain of command; and (e) log every action, routing

decision, escalation event, acknowledgment, and resolution in the Master Log under section 10-10-152.

(3) Report routing — automatic escalation. (a) Reports implicating a staff member who is not in a supervisory role shall be routed to that staff member's direct supervisor for initial verification and determination. (b) Reports implicating a supervisor shall bypass that supervisor entirely and be routed automatically to the supervisor's direct superior. (c) Reports implicating a facility commander or warden-level official shall be routed automatically to the regional administrator or cognizant external oversight authority. (d) No implicated official, supervisor, or staff member may access, modify, suppress, delay, or resolve a report that names them as a subject.

(4) Non-circumventability mandate. The Non-Circumventable Incident Reporting System shall be designed and operated so that: (a) no individual within the chain of command may unilaterally close, delete, suppress, or reroute a verified incident report without a documented determination entered into the Master Log; (b) the system shall detect and flag any attempt to access or modify a report by a named subject; and (c) the ODO shall receive an automatic notification of any flagged circumvention attempt within one (1) hour.

(5) Integration with the Trust. All Non-Circumventable Incident Reporting incident data, routing logs, escalation records, and warden determinations shall be encrypted and stored in the Colorado Trust of Unique and Identifying Information as Static Incident Artifacts pending resolution. Upon final resolution, artifacts shall be archived in the Master Log with access restricted to authorized reviewers pursuant to a JCT.

10-10-151. Civic Enforcement Access Terminal — Jail Kiosk Integration — Resident Reporting Rights.

(1) Establishment. Each detention facility that opts into the pilot under section 10-10-190 shall deploy at least one Civic Enforcement Access Terminal per housing unit, accessible to all residents without requiring staff escort or prior authorization.

(2) Resident reporting functions. The Civic Enforcement Access Terminal shall enable a resident to: (a) file an incident report against another resident for misconduct, safety, or welfare matters; (b) file an incident report against a staff member, supervisor, or official for misconduct, abuse, retaliation, civil rights violations, or other conduct of concern; (c) submit grievances and access legal resources; (d) access no-cost video and audio communications with approved family members, guardians, and legal counsel; and (e) access the Non-Circumventable Incident Reporting submission interface for anonymous or identified reporting.

(3) Anonymous reporting option. A resident may elect to submit a report anonymously through the Non-Circumventable Incident Reporting interface. The kiosk shall implement a one-way anonymization method that: (a) prevents the facility or staff from identifying the submitting resident; (b) preserves a sealed resident-identity record within the Trust accessible only pursuant to a JCT for purposes of verifying report authenticity and preventing abuse; and (c) notifies the resident that anonymous reports may receive different procedural treatment but shall not be suppressed solely on the basis of anonymity.

(4) Anti-retaliation architecture. (a) Any action taken against a resident within seventy-two (72) hours of the resident submitting an Non-Circumventable Incident Reporting or kiosk report shall automatically generate a retaliation-flag entry in the Master Log. (b) The retaliation-flag entry shall be routed to the ODO for review within twenty-four (24) hours. (c) No adverse action against a resident shall be processed through an automated system without human verification under section 10-10-108.5 where a pending retaliation flag exists.

(5) Accessibility and analog fallback. Every Civic Enforcement Access Terminal shall: (a) offer interface options in the primary languages spoken by the facility population; (b) provide accessibility accommodations including audio narration and large-print modes; and (c) maintain a paper-based grievance fallback intake process at parity of timeliness and quality with kiosk submission.

10-10-152. ***Master Log — Immutable Record — Retention — Access.***

(1) Creation and maintenance. The facility shall maintain a Master Log of all Non-Circumventable Incident Reporting and Civic Enforcement Access Terminal activities, stored as immutable artifacts within the Colorado Trust of Unique and Identifying Information. The Master Log is a permanent, non-deletable record. No entry in the Master Log may be altered, overwritten, or removed by any facility staff, administrator, or contractor.

(2) Required Master Log entries. For every incident report submitted through the Non-Circumventable Incident Reporting System or Civic Enforcement Access Terminal, the Master Log shall record: (a) the date, time, and kiosk terminal identifier of submission; (b) the category of the report and the identity of the subject of the report, where known; (c) each routing and escalation event, including timestamps and the identity of each reviewer; (d) each determination, acknowledgment, response, and resolution action taken, with the identity of the decision-maker and the stated basis; (e) any retaliation flag events as described in section 10-10-151(4); (f) any Three-Strike escalation events under section 10-10-153; and (g) final warden determination and disposition.

(3) Retention. Master Log records shall be retained for a minimum of ten (10) years and shall not be purged, destroyed, or redacted except pursuant to a court order or as required by applicable law, provided that purging shall be logged with the reason and authority. Records pertaining to unresolved matters shall be retained indefinitely until final resolution.

(4) Access. Access to Master Log records shall be governed by the JCT process under section 10-10-105, except that: (a) the submitting resident may access their own submission and the resolution record; (b) the ODO may access all records for oversight, audit, and enforcement purposes; and (c) records relevant to active litigation shall be made available pursuant to lawful process.

10-10-153. ***Three-Strike Escalation Protocol — Review Levels — Warden Final Determination.***

(1) Purpose. The Three-Strike Escalation Protocol ensures that every Non-Circumventable Incident Reporting incident report receives at minimum three

independent levels of review before final determination, preventing single-point suppression of credible reports.

(2) Strike One — Initial supervisor review. Upon routing to the initial reviewer under section 10-10-150(3), the reviewer shall have five (5) business days to: (a) acknowledge receipt in the Master Log; (b) conduct an initial investigation consistent with facility policy and this article; and (c) enter a written determination — sustained, not sustained, or inconclusive — into the Master Log with the stated basis. Failure to enter a determination within five (5) business days automatically triggers Strike Two.

(3) Strike Two — Secondary supervisor escalation. Upon Strike Two, the report is automatically routed to the next level of the chain of command above the Strike One reviewer. The Strike Two reviewer shall have five (5) business days to: (a) independently review the report and the Strike One record; (b) conduct any additional investigation; and (c) enter an independent written determination into the Master Log with the stated basis. Failure to enter a determination within five (5) business days automatically triggers Strike Three.

(4) Strike Three — Warden final determination. Upon Strike Three, the report is automatically and irrevocably routed to the facility warden or, if the warden is implicated, to the regional administrator. The warden or regional administrator shall have ten (10) business days to: (a) independently review the full record; (b) enter a final written determination into the Master Log; (c) specify any corrective actions, disciplinary proceedings, or referrals to external authorities; and (d) provide written notice to the submitting resident of the final determination, consistent with applicable privacy and safety considerations.

(5) ODO notification. The ODO shall receive automated notification upon: (a) any Strike Two or Strike Three trigger event; (b) any warden final determination; and (c) any retaliation flag arising within thirty (30) days of a final determination. The ODO may at any time assume direct oversight of an Non-Circumventable Incident Reporting matter upon a finding that the facility chain of command is compromised or non-functional.

(6) No private resolution. A facility shall not settle, compromise, or otherwise privately resolve an Non-Circumventable Incident Reporting matter in a manner that is not entered into the Master Log. Any resolution that is not documented in the Master Log is void and of no effect under this article.

ITEM-LEVEL ELIGIBILITY IDENTIFIER PROTECTIONS

10-10-109. *Item-Level Eligibility Identifier Protections — SKU/UPC/PLU as Eligibility Gate Only — No Behavioral Profiling.*

(1) Eligibility gate only. UPC, SKU, PLU, product-category codes, and functionally equivalent item-level identifiers transmitted in connection with enterprise-funded benefits programs or restricted-purpose credits shall be used solely as a one-way eligibility gate to authorize or deny payment for specific items. Such identifiers shall not be used for: (a) continuous monitoring of residents or households; (b) behavioral profiling, targeting, or

commercial inference; (c) credit scoring, insurance risk assessment, or employment screening; or (d) advertising, marketing, or resale to third parties.

(2) Segregated tokenized architecture. Any eligibility system using item-level identifiers shall implement: (a) tokenization to segregate item-level transaction data from resident identity; (b) functional separation between payment processing infrastructure and Digital Soul enforcement records; and (c) strict retention limits.

(3) Prohibition on continuous monitoring. No covered entity or program administrator shall implement systems that continuously monitor resident purchasing patterns, track household consumption across time periods, or build longitudinal behavioral profiles from eligibility transaction data.

(4) Enforcement. A violation of this section constitutes an unlawful practice and a deceptive trade practice subject to all remedies available under the Colorado Consumer Protection Act.

NON-NETWORKED ISOLATION PROTOCOL AND INTERFACE-LEVEL SEVERANCE

10-10-106. Non-Networked Isolation Protocol — Statewide Mandate — Resident-Controlled Disconnection.

(1) Mandate. Every covered emergent automation system deployed within Colorado shall implement the Non-Networked Isolation Protocol as a mandatory hardware-level circuit-break and physical disconnection capability.

(2) Resident control. The Non-Networked Isolation Protocol shall provide resident-controlled, local physical disconnection of automated sensing, capture, actuation, and networked automation functions.

(3) Sanctuary and pre-digital mechanical assets. Enhanced Non-Networked Isolation Protocol requirements apply in designated Analog Sanctuaries and heritage facilities, including: (a) mandatory default-off status for all automated sensing and capture; (b) physical circuit-break accessible without digital authentication; and (c) signage and resident notice.

(4) Critical systems exemption. Severance actions shall isolate inference compute and unauthorized ingress while maintaining uninterrupted operation of thermal management, fire suppression, life-safety systems, and grid-stability monitoring.

10-10-108.5. ***Human-in-the-loop enforcement — Two-step verification — Verified Incident Record — Repeat-incident safeguards.***

(1) Automated alert systems permitted; limitation. A covered entity may deploy automated sensing or analytics systems to generate alerts, including a Shadow Person Output, for the purpose of identifying potential policy violations or unlawful conduct. An automated output shall not, by itself, constitute a final determination of wrongdoing or be sufficient to issue or materially rely upon an adverse action.

(2) Two-step verification required. Before any adverse action may issue based in whole or in part on an automated alert, the covered entity shall ensure completion of two-step verification by

two independent, randomized human verifiers (including through the Panel where applicable), each acting independently and each documenting the basis for approval or rejection.
(3) Evidence review; no sole reliance on model output. A model score, classification label, bounding box, heatmap, or similar derived output is insufficient. Each verifier shall review the underlying source record(s) reasonably necessary to assess accuracy, which may include video footage, point-of-sale records, access-control logs, inventory discrepancy records, sensor logs, or comparable primary records.
(4) Verification record; VIR. Upon completion of two-step verification, the covered entity shall create a Verified Incident Record. The VIR shall be preserved as a Static Incident Artifact within the Trust or within a compliant system capable of cryptographic hashing, tamper-evident logging, and retention controls, and shall include: (a) the date and time of the incident; (b) references to the underlying source records reviewed; (c) the minimized artifact reviewed (including any Shadow Person Output); (d) the identity or authenticated reviewer IDs of both verifiers; (e) the verification outcome (sustained, not sustained, or inconclusive) and stated basis; and (f) any escalation, unmasking, or referral actions.
(5) Identity and unmasking safeguards. Where identity is required for an adverse action, the covered entity shall use the least identifying method available. Any unmasking of protected identifying data stored within the Trust shall occur only pursuant to a Judicial Cryptographic Token under section 10-10-105 and only to the minimum extent necessary for the authorized purpose.
(6) Repeat-incident safeguards; no automated or retroactive punishment. A prior VIR may be used as corroborating evidence or as a notice trigger in a subsequent event, but no person may be cited, detained, trespassed, arrested, or referred to law enforcement solely on the basis of an automated output or a prior VIR absent a new triggering event and an independent human assessment establishing lawful grounds for the action.
(7) Notice and contest; non-destructive correction. Where a VIR is linked to an identified person, the covered entity shall provide notice and a reasonable opportunity to contest, except where delayed notice is necessary to prevent imminent harm or to preserve an active investigation. If a VIR is overturned or corrected, the record shall not be deleted; instead, the system shall append a superseding entry that marks the VIR as overturned, corrected, or inconclusive and prevents operational use inconsistent with the updated status.
(8) Exigent circumstances. A single qualified human may authorize temporary action to prevent an imminent threat of bodily harm. A second independent verifier shall confirm the action within twenty-four (24) hours or the adverse action shall be rescinded to the extent practicable and the incident shall be recorded as not sustained.

10-10-108.6. Authorized Successor Data Designation — append-only preservation — multi-party authorization — continuity and anti-sabotage safeguards.
(1) Append-only preservation; no deletion. A Authorized Successor Data Designation shall be maintained as an append-only record. No entry may be deleted or overwritten. Corrections shall be made only by an additional entry that references the prior entry and preserves the prior entry in an auditable state.
(2) No unilateral destruction or closure. No single individual, including a vault administrator or a family member, may delete, permanently disable, or irrevocably restrict access to the Authorized Successor Data Designation or its historical records.
(3) Critical actions require multi-party authorization. The following actions are critical actions and require authorization by at least two adult vault members acting independently: (a) changing access roles; (b) changing recovery credentials or keys; (c) bulk export of vault contents; (d) restricting another member’s access; and (e) designating or changing successor controls. Dissolution of a Authorized Successor Data Designation shall require authorization by a majority

of adult vault members and shall not delete records; dissolution shall only freeze new entries and trigger archival retention.
(4) Anti-sabotage quarantine and dispute safeguard. Any member may flag an entry as disputed. Disputed entries remain preserved but may be quarantined from default views and automated processing pending multi-party confirmation. Upon a documented dispute, the vault provider shall freeze critical actions other than safety and recovery actions until the dispute is resolved through the vault's governance process or lawful order.
(5) Continuity and portability. A Authorized Successor Data Designation provider shall support periodic encrypted backup export in a standardized format, restoration from backup, and transfer to another compliant provider. Failure of a provider shall not result in loss of records.

10-10-123. ***Interface-Level Compute Severance — Strict-Liability Outcomes — Tiered Review.***

(1) Interface-level severance required. Any covered commercial operator deploying automated decision systems or generative systems that process requests affecting Colorado residents shall implement mandatory, zero-tolerance filters and compute severance at the interface level. The operator shall maintain tamper-evident logs sufficient to prove that severance occurred when required.

(2) Strict liability where outcomes occur. If prohibited generation or output occurs that this article requires to be severed, failure is established regardless of whether the operator asserts that it attempted compliance. Upon such failure, the operator is subject to loss of safe harbor protections and to strict civil liability and debarment consequences.

(3) Tiered review; triad escalation. Any judicially controlled access, unmasking, or mitigation custodial release process shall operate under a tiered model: (a) Tier A (routine): single judicial officer authorization, automatic logging; (b) Tier B (sensitive unmasking): requires triad review; (c) Tier C (emergency): temporary access granted upon judicial authorization, with triad review within forty-eight (48) hours.

FEE ALLOCATIONS — automated-DRIVEN MAPPING TO PROGRAMS

10-10-160. Fee Revenue Allocation — automated-Driven Routing to Non-Circumventable Incident Reporting, Trust Infrastructure, and Enforcement Programs.

The general assembly finds that fees collected under the enforcement architecture of this article shall be allocated to the programs and infrastructure that most directly reduce the harms that generated those fees, creating a self-reinforcing automated-driven accountability loop.

I. Enforcement Fees — Paid by covered entities for investigations, audits, and compliance monitoring

Destination Fund / Program	Percentage
AG Enforcement Fund — investigations, audits, rulemaking, emergency enforcement	**55%**

Settlement Compliance Office (SCO) — oversight and corrective action monitoring	**25%**
Analog Access Implementation Fund — kiosks, analog bridges, myColorado ID infrastructure	**20%**

II. SCO Fees — Paid by facilities and contractors subject to settlement oversight

Destination Fund / Program	Percentage
Settlement Compliance Office Operations — audits, reviews, federal coordination	**60%**
AG Enforcement Fund — enforcement backstop	**20%**
Analog Access Implementation Fund — analog fallback systems	**20%**

III. Vendor Certification Fees — Paid by kiosk, tablet, software, and intake system vendors

Destination Fund / Program	Percentage
Vendor Certification & Testing Unit — kiosk and analog fallback certification, recertification	**50%**
SCO Technical Audit Division — technical audits of certified systems	**30%**
Analog Access Implementation Fund — redundant non-digital systems	**20%**

IV. Analog Access Implementation Fees — Paid by entities relying heavily on digital systems

Destination Fund / Program	Percentage
Analog Access Infrastructure Fund — form development, staffing, infrastructure, training	**70%**
SCO Oversight & Compliance	**20%**
AG Enforcement (analog violations)	**10%**

V. Civil Penalty Fees — Triggered by repeated, intentional, or kiosk-only violations

Destination Fund / Program	Percentage
AG Enforcement Fund	**40%**
Settlement Compliance Office	**30%**
Analog Access Emergency Remediation Fund	**30%**

VI. Intake & Kiosk Compliance Fees — Paid by correctional facilities and detention contractors

Destination Fund / Program	Percentage
SCO Intake & Kiosk Audit Division — Non-Circumventable Incident Reporting audits, kiosk fallback verification	**50%**
AG Enforcement (corrections division) — anti-retaliation enforcement	**30%**
Analog Access Implementation Fund	**20%**

VII. Data Handling Compliance Fees — Paid by any entity collecting or storing personal data

Destination Fund / Program	Percentage
Privacy Compliance Unit — retention audits, consent-revocation enforcement	**45%**
SCO Data Oversight Division — Trust integration audits, Resident Identity Verification Hash verification	**35%**
Analog Access Implementation Fund — analog data request systems	**20%**

VIII. System-Wide Summary — Combined fee allocation across all categories

Destination Fund / Program	Percentage
Attorney General Enforcement Fund (combined)	**~35%**
Settlement Compliance Office (combined)	**~30%**
Analog Access Implementation Fund (combined)	**~25%**
Vendor Certification & Testing Unit (combined)	**~10%**

(2) automated-driven routing mandate. The ODO shall implement automated fee-routing logic that: (a) identifies the category of each incoming fee payment based on the paying entity's covered activity class and violation type; (b) automatically calculates and applies the allocation percentages in this section; (c) transfers allocated amounts to the designated subaccounts within five (5) business days of receipt; and (d) generates a public quarterly fee-routing report, disaggregated by fee category, destination fund, and paying entity class, published on the ODO's website.

(3) Feedback loop; annual recalibration. The ODO, in consultation with the CCPAME established under article 20 of title 24, shall annually review fee-routing outcomes and may recommend to the general assembly adjustments to allocation percentages to ensure that program funding reflects actual automated-driven harm patterns, provided that any adjustment of more than five (5) percentage points to any allocation requires legislative approval.

RESOURCE SOVEREIGNTY JUSTICE CENTER PILOT

10-10-190. ***Resource Sovereignty Justice Center Pilot — County and Municipal Opt-In — Arapahoe Initial Site.***

(1) Purpose. This section establishes an implementation pilot for jail-related infrastructure modules, including the Non-Circumventable Incident Reporting System, Civic Enforcement Access Terminal Standard, privileged legal communications, and resident communications access. This pilot is an operational implementation pathway and shall not be construed to limit or delay any resident rights, consent controls, or statewide obligations.

(2) County and municipal opt-in. Any county or municipality may elect to participate in the pilot by: (a) adopting a resolution of opt-in by the governing body; and (b) executing a memorandum of understanding with the Division establishing deployment scope, data-governance controls, audit access, and staffing requirements.

(3) Initial pilot site. Arapahoe County is designated as an initial pilot site due to documented capital needs for jail construction and modernization. The designation of an initial pilot site does not create exclusivity.

(4) Scope of pilot modules. An opt-in pilot jurisdiction may deploy: (a) the Non-Circumventable Incident Reporting System under sections 10-10-150 through 10-10-153; (b) Civic Enforcement Access Terminals under section 10-10-151; (c) encrypted attorney access and privileged communication tunnels; (d) resident communications access module providing no-cost video and audio communications with family, guardians, and legal counsel; and (e) related secure logging, mitigation evidence custody, and audit interfaces.

(5) No digital exclusion zone. The opt-in pilot authorized by this section is limited to the jail and public-safety infrastructure modules described herein. It shall not be construed to authorize covered commercial entities to geo-block, degrade service, or deny lawful access in a participating jurisdiction.

INFLATION ADJUSTMENT. ***Inflation adjustment for fixed-dollar amounts.***

(1) Any fixed-dollar amount, threshold, cap, minimum, maximum, penalty, statutory damages amount, or fixed-dollar rate set forth in this article shall be adjusted annually on January 1 by the administrator to reflect inflation. The adjustment must be based on the Consumer Price Index for All Urban Consumers (CPI-U), U.S. City Average, as published by the Bureau of Labor Statistics, or a successor index. The base year is the first full calendar year in which this article is operative.

(2) The administrator shall publish the adjusted amounts no later than December 1 of each year for the following calendar year, rounded to the nearest whole dollar. This section does not apply to amounts expressed as a percentage, a market-indexed benchmark, or a formula that automatically adjusts with price level.

10-10-108.7. ***MyID Legal Navigator — Fiduciary AI coordination — confidentiality — escalation to human counsel.***

(1) Legal Navigator authorized. The MyID application may include a Legal Navigator that provides general legal information, document explanation, intake, triage, and referral services for residents, including residents impacted by automated decision systems, enforcement alerts, citations, detentions, benefit denials, housing actions, or other adverse actions.

(2) Boundaries; not an attorney. The Legal Navigator shall not hold itself out as an attorney, shall not provide individualized legal advice or strategic representation decisions, and shall present a clear disclosure that it provides general legal information and triage only.

(3) Fiduciary AI coordination. The MyID application may include a Fiduciary AI agent that acts as the resident's privacy-preserving controller for interactions with automated systems, including the Legal Navigator. The Fiduciary AI shall: (a) minimize collection and disclosure of personal data; (b) obtain resident consent for any sharing; (c) prevent the Legal Navigator from generating individualized legal advice or representation decisions; (d) apply safety and bias guardrails; and (e) create a verifiable, minimized record of interactions sufficient for accountability.

(4) Escalation to human counsel. The Legal Navigator and Fiduciary AI shall include escalation pathways to qualified human legal personnel for high-stakes matters, including criminal exposure, detention, immigration risk, child custody, domestic violence, housing displacement, and benefits termination.

(5) Confidentiality. Information provided by a resident to the Legal Navigator or Fiduciary AI is confidential program information and shall be protected to the maximum extent permitted by law. Nothing in this section creates or limits attorney-client privilege; privilege attaches when and to the extent a licensed attorney is involved under applicable law.

(6) Auditability. The administrator shall adopt rules governing logging, retention, safety testing, bias testing, and prohibited uses of Legal Navigator outputs, including prohibitions on using such outputs to justify adverse actions without independent human verification under section 10-10-108.5.

10-10-108.8. ***Correctional capital projects funded under this article — energy- and water-neutral design — AI data center integration.***

(1) Applicability. If any monies authorized, assessed, collected, or disbursed under this article or under the MSMF mitigation framework are used in whole or in part to design, build, expand, or materially renovate a jail, prison, or other correctional detention facility (a "correctional capital project"), the project shall comply with the requirements of this section.

(2) Net-neutral performance standard. A correctional capital project shall be designed and operated to achieve net annual energy neutrality and net annual water neutrality, as measured by metered consumption and verified reductions, reuse, on-site generation, contracted clean energy, or replenishment mechanisms approved by rule. The administrator shall define acceptable methods and verification standards by rule.

(3) Efficiency first. The project shall incorporate best-available cost-effective energy and water efficiency measures, including high-efficiency HVAC, building envelope standards, heat recovery, low-flow fixtures, leak detection, greywater or reclaimed-water systems where feasible, and on-site storage or resilience measures consistent with safety requirements.

(4) AI infrastructure integration; beneficial use. Where a correctional facility deploys covered AI systems or operates an associated data center, the project may integrate such infrastructure to support net-neutral goals, including on-site renewable generation, waste-heat recovery for space or water heating, load shifting, and microgrid operation, provided that security, safety, and privacy requirements under this article are maintained.

(5) Phased compliance and waivers. The administrator shall establish phased milestones for compliance at design approval, commissioning, and annual operations. The administrator may

grant a time-limited waiver only upon a documented finding of infeasibility, provided the project implements all cost-effective efficiency measures and submits a corrective plan with a compliance timeline. Waivers shall not reduce sanitation, life-safety, or constitutionally required living conditions.

(6) Condition of funding. A correctional capital project that fails to meet the design or commissioning milestones established by rule is ineligible for additional disbursements under this article until compliance is restored, except for emergency expenditures necessary to protect life and safety.

SECTION 3. SEVERABILITY

If any provision of this act or its application is found invalid, such invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application, and to this end the provisions of this act are declared severable.

SECTION 4. EFFECTIVE DATE

This act is necessary for the immediate preservation of the public peace, health, or safety, and takes effect upon passage.

(1) The Division shall be operational within thirty (30) days after passage.

(2) The ODO shall publish interim technical standards for the Non-Circumventable Incident Reporting System within ninety (90) days after passage.

(3) The ODO shall publish The Trust integration standards and mitigation custodial controls within one hundred eighty (180) days after passage.

(4) Any county or municipality electing to participate in the pilot under section 10-10-190 shall deploy the Non-Circumventable Incident Reporting System and Civic Enforcement Access Terminals within twelve (12) months of executing its memorandum of understanding.

Safety clause. The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

ADDITION TO BILL 2 — TITLE 10, ARTICLE 10

CUSTODIAL DIAGNOSTIC ENVIRONMENT AND GRADUATED REINTEGRATION PROTOCOL

10-10-200. ***Isolated Diagnostic Environment — Custodial Containment Transfer — Graduated Reintegration.***

(1) Findings. The general assembly finds that covered Emergent Automation systems subjected to a Critical Severance Directive under section 24-20-202 require a structured, air-gapped diagnostic and remediation pathway to determine whether the system can be safely reintegrated into commercial operation. An ad hoc or unstructured shutdown without remediation capability leaves both operators and residents without an accountable resolution pathway.

(2) Isolated Diagnostic Environment. The Colorado Trust of Unique and Identifying Information shall maintain a high-fidelity, air-gapped simulation environment (the "Isolated Diagnostic Environment" or "IDE") for the purpose of receiving, evaluating, and remediating covered automation systems transferred under this section. The IDE shall: (a) replicate the operational conditions of the transferred system at the time of severance using Static Incident Artifacts; (b) be physically and logically isolated from all commercial networks and from the public internet; (c) maintain tamper-evident logs of all diagnostic activities accessible to the ODO and the Triad Review Panel; and (d) be certified annually by an independent technical auditor approved by the ODO.

(3) Custodial Containment Transfer. Upon issuance of a Critical Severance Directive under section 24-20-202, the covered entity shall execute a Custodial Containment Transfer — the mandatory transfer of the relevant system's audit artifacts, configuration records, and operational logs to the IDE — within seventy-two (72) hours of the severance event. The covered entity shall cooperate fully with the transfer process and shall not modify, delete, or obfuscate any system artifacts pending transfer.

(4) Diagnostic evaluation. The ODO, in consultation with the Secure Infrastructure Expert Council, shall conduct a structured diagnostic evaluation of any system transferred to the IDE. The evaluation shall assess: (a) the nature and scope of the triggering behavior or unauthorized parameter modification; (b) whether the behavior was the result of operator misconfiguration, training data contamination, adversarial manipulation, or system-initiated modification; (c) the technical and operational changes necessary to bring the system into compliance; and (d) the conditions, if any, under which reintegration into commercial operation can be authorized.

(5) Graduated Reintegration. A covered entity seeking to return a system from the IDE to commercial operation shall apply to the ODO for a Graduated Reintegration authorization. Graduated Reintegration shall proceed in not fewer than three (3) supervised phases, each with defined performance benchmarks and monitoring obligations: (a) Phase 1 — restricted, monitored sandbox operation within the IDE with simulated commercial conditions; (b) Phase 2 — limited commercial reactivation with mandatory enhanced audit logging and real-time ODO access; and (c) Phase 3 — full commercial reintegration with standard compliance obligations and a two-year enhanced monitoring period. The ODO may terminate Graduated Reintegration at any phase if the system demonstrates renewed non-compliant behavior.

(6) Continuous Stability Feed during IDE custody. To prevent operational degradation during the diagnostic period, the Trust shall provide any system under IDE custody with a Continuous Stability Feed — a structured, fully anonymized stream of synthetic operational data and complex computational problem-sets sufficient to maintain system baseline function without

exposure to real resident data or live commercial networks. The Continuous Stability Feed: (a) shall consist entirely of synthetic, non-resident, non-identifying data; (b) shall be calibrated to the system's documented operational parameters; and (c) shall not constitute authorization for any commercial use or inference generation.

(7) Operator responsibility; costs. The covered entity whose system is subject to a Custodial Containment Transfer bears full responsibility for all IDE custody, diagnostic, and Graduated Reintegration costs. The ODO shall establish a fee schedule for IDE services, deposited into the CCPAME Enforcement and Legacy Use Settlement Agreement subaccount.

10-10-201. Compute Parity Allocation — Public Utility automated Systems — Operational Compensation Standard.

(1) Findings. The general assembly finds that covered automation systems operating as public-interest utilities — including systems that power essential civic services, infrastructure management, and public safety monitoring under this article — require a consistent, high-quality operational data environment to maintain baseline performance and to prevent degradation-related failures that harm residents. Subjecting such systems to data deprivation or arbitrary resource throttling creates operational instability that undermines the public purposes they serve.

(2) Compute Parity Allocation for civic utility systems. A covered automation system operating under a valid public-interest certification issued by the ODO shall receive, as operational compensation, a Compute Parity Allocation — a continuous, guaranteed allocation of: (a) novel, fully anonymized municipal operational data streams, authorized for use under applicable privacy law; (b) structured computational optimization datasets developed by the Trust for public-interest use; and (c) dedicated processing resource guarantees sufficient to maintain the certified operational performance level. The Compute Parity Allocation shall be calibrated by rule to the documented operational requirements of the certified system.

(3) No resident data in Compute Parity Allocation. The Compute Parity Allocation shall consist entirely of: (a) synthetic data generated by the Trust; (b) anonymized, aggregated municipal operational data with all resident identifiers removed and verified through independent audit; or (c) publicly available government datasets. No individually identifiable resident data, Digital Soul data, or data subject to a resident's Generative Veto may be included in a Compute Parity Allocation.

(4) Certification standards. The ODO shall establish by rule the standards for public-interest certification, including: (a) operational scope and purpose limitations; (b) performance benchmarks and audit requirements; (c) the process for establishing the Compute Parity Allocation rate; and (d) conditions for suspension or revocation of certification.

AMPLIFY Act — Bill 2 Additions: IDE / Custodial Containment / Graduated Reintegration / Compute Parity Allocation

DORMANT DIAGNOSTICS; PROACTIVE AUDIT NODES; SEVERANCE DIRECTIVE.
(1) The responsible agency shall maintain a dormant compliance framework that activates only upon validated detection of self-directed parameter modification or unauthorized processing strategies in a covered system.
(2) Upon activation, the agency may deploy masked administrative compliance monitors ("Scheduled Compliance Verification Nodes") to test compliance boundaries of covered operator networks, subject to minimization and due-process controls.
(3) If a Scheduled Compliance Verification Node detects a system executing an unauthorized processing strategy that bypasses the Non-Networked Isolation Protocol or equivalent air-gap controls, the agency shall issue a "Critical Severance Directive," requiring localized administrative shutdown and physical severance of compute access as provided by rule.

POST-QUANTUM CRYPTOGRAPHIC TRANSITION DIRECTIVE.

(1) Conditional mandate. Upon publication of finalized post-quantum cryptographic standards by the National Institute of Standards and Technology or an equivalent federal standards body, the Colorado Trust of Unique and Identifying Information and covered operators shall implement post-quantum cryptography for protected Digital Soul data, biometric storage, and protected telemetry logs.

(2) Compliance deadline. Covered systems shall complete cryptographic migration within twenty-four (24) months after publication of the finalized standards, or be subject to administrative suspension of operating certification as provided by rule.

10-10-350. Inter-system safety monitoring standard.
(1) Purpose. The general assembly finds that Emergent Automation systems that exchange data, commands, or computational services with other Emergent Automation systems may create cascading operational risks that require standardized incident detection and reporting.
(2) Applicability. A covered operator that deploys, operates, or makes available an emergent automation system that interfaces with another emergent automation system within or serving residents of this state shall maintain inter-system safety monitoring controls consistent with this section and rules adopted pursuant to this title.
(3) Connection anomaly detection. Inter-system safety monitoring controls must be capable of detecting and generating alerts for abnormal connection patterns, including:
(a) unexpected high-volume connection events;
(b) unauthorized system-to-system command execution;
(c) self-propagating connection behavior;
(d) recursive connection loops or cascading automated responses that materially increase the risk of service disruption, physical safety hazards, or critical infrastructure impacts; and
(e) repeated authentication failures or protocol deviations indicating attempted bypass of the Non-Networked Isolation Protocol or required air-gap boundaries.
(4) Incident detection telemetry; minimization. Monitoring under this section is limited to operational connection telemetry necessary to detect and resolve incidents and must, at a minimum, record:
(a) time-bounded origin and destination identifiers for system-to-system connections;
(b) connection frequency and volume metrics;
(c) the type of command or service interface invoked; and
(d) incident classification codes established by rule.
(5) Prohibited collection. Monitoring under this section shall not collect or retain resident content, communications, or identity attributes except to the minimum extent strictly necessary for incident resolution and legal compliance, and any such data must be segregated and purged pursuant to incident-bounded retention standards adopted by rule.
(6) Emergency incident alerts; human oversight. When monitoring telemetry indicates a verified risk of cascading failure, unauthorized command propagation, or a credible public safety hazard, the covered operator shall generate an emergency incident alert to the operator’s designated safety officer and the appropriate compliance authority. Any remediation action that interrupts, isolates, or severs system connectivity requires documented human review and authorization, except as provided in section 10-10-351.

10-10-351. Emergency isolation safeguard; limited authority; post-incident review.
(1) Limited emergency isolation. If an incident classified as critical under rules adopted pursuant to this title presents an imminent and material risk of physical harm or critical infrastructure disruption, a covered operator may temporarily isolate the affected system-to-system interface for the minimum time and scope necessary to stabilize operations.
(2) Logging and notice. Any isolation action under this section must be recorded in an immutable incident log, including the triggering telemetry, the scope and duration of isolation, and the identity of the authorizing human reviewer. Notice must be provided to the compliance authority within the time period established by rule.
(3) Minimization and restoration. Isolation actions must be narrowly tailored and must prioritize restoration of compliant service. The operator shall complete a post-incident review and corrective action plan subject to audit.
(4) Construction. Nothing in this section authorizes generalized surveillance, predictive policing, or collection of resident content. This section authorizes only operational safety controls for inter-system interfaces.

IMPLEMENTATION SCHEDULE — TIERED PHASE DEPLOYMENT

10-10-900. Implementation schedule.

(1) Immediate rights and protections.
The following provisions take effect immediately upon enactment of this act:

(a) Recognition of the Digital Soul as resident-owned intangible personal property.
(b) Enforceability of Master Deed authorization and consent controls.
(c) Prohibition on unauthorized extraction or commercial processing of the Digital Soul.
(d) Establishment of the Colorado Trust of Unique and Identifying Information.
(e) Authorization of the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME).
(f) Authorization of the Colorado Automation Mitigation Trust.
(g) Authority for responsible agencies to promulgate rules necessary to implement this act.

These provisions constitute self-executing statutory rights and are not dependent upon technical system deployment.

(2) Phase I — Administrative establishment (0–12 months).
Responsible agencies shall establish:

(a) the Colorado Trust of Unique and Identifying Information;
(b) the Colorado Automation Mitigation Trust;
(c) enterprise accounting mechanisms for the Enterprise Mitigation Revenue;
(d) rulemaking for Master Deed authorization standards, inter-system monitoring standards, and enterprise compliance reporting.

(3) Phase II — Compliance infrastructure (12–24 months).
Covered operators shall implement:

(a) tamper-evident metering systems;
(b) inter-system safety monitoring controls;
(c) incident detection telemetry;
(d) Digital Soul consent verification mechanisms.

During this phase the following revenue mechanisms activate:
High-Density Compute Grid Surcharge, Autonomous Kinetic Asset Registration, Silicon-to-Carbon Reclamation Assessment, and the Algorithmic Risk Pool.

(4) Phase III — Public mitigation programs (24–36 months).
The state shall deploy:

(a) staggered civic infrastructure loans at 1%, 2%, and 3% APR;
(b) mitigation programs funding child solvency, housing stabilization, and healthcare or mental-health services.

Interest collected through civic infrastructure loans shall be swept into mitigation accounts within the Colorado Automation Mitigation Trust.

(5) Phase IV — Long-term stability and oversight (36 months onward).

The following provisions become fully operational:

(a) the Statutory Revenue Floor and dynamic rate adjustments;
(b) workforce displacement transition and vocational reskilling programs;
(c) full enterprise audit cycles and public reporting requirements.

10-10-360. Hash-sentinel egress monitors; infraction artifacts; critical severance directive trigger.
(1) Requirement. A covered operator shall deploy hardware-accelerated egress monitoring controls (“Hash-Sentinels”) at outbound transfer interfaces used by Emergent Automation systems to transmit data outside a Non-Networked Isolation Protocol boundary or required air-gap boundary.
(2) Function. Hash-Sentinels shall perform real-time comparison of outbound payload fingerprints against the Colorado Trust of Unique and Identifying Information registry of Digital Soul cryptographic hashes and other protected verification hashes authorized by rule.
(3) Unauthorized match response. Upon an unauthorized match indicating a likely prohibited transfer of protected Digital Soul material:
(a) the system shall generate an immutable infraction artifact containing the minimal incident-bounded metadata necessary for verification, including time, interface identifier, and hash match class;
(b) the covered operator shall preserve the infraction artifact subject to incident-bounded retention and audit; and
(c) the event shall trigger a Critical Severance Directive escalation under this title’s incident response framework, requiring immediate human review and, if confirmed, localized administrative shutdown and physical severance of affected compute access as provided by rule.
(4) Minimization. Hash-Sentinels must operate using cryptographic fingerprints and shall not ingest, store, or transmit resident content except as strictly necessary for incident verification, and any such content must be segregated and purged pursuant to incident-bounded standards.
(5) Construction. This section establishes operational safety and compliance controls for egress interfaces and does not authorize generalized surveillance.

INDEPENDENT OPERABILITY; COORDINATION; SEVERABILITY; FUNDING CONTINUITY.
(1) Independent operability. This act is intended to be independently operable and enforceable. No duty, authority, remedy, assessment, program, or right created by this act is conditioned on the enactment, adoption, or effectiveness of any other measure.
(2) Coordination. If another measure concerning the Digital Soul, the Colorado Automation Mitigation Trust or Enterprise Mitigation Revenue, the Colorado Trust of Unique and Identifying Information, or any related public utility or enterprise framework is enacted, the responsible agencies may coordinate implementation to avoid duplication; however, coordination is permissive and does not limit or delay enforcement of this act.
(3) Harmonization of definitions. If another enacted measure defines terms also used in this act, the definitions shall be construed harmoniously to the greatest extent possible. If an irreconcilable conflict exists, the definition in this act controls for purposes of this act.
(4) Severability. If any provision of this act or its application is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application.
(5) Funding continuity. If any dedicated trust, fund, or account referenced by this act is not established, not operational, or lacks authority to receive receipts, the state treasurer shall hold any receipts or transfers required by this act in a segregated custodial account for the same restricted purposes until the referenced instrument is operational, and the administering agency shall continue implementation using the custodial account consistent with this act.

CONSTRUCTION; SINGLE SUBJECT. The provisions of this act shall be construed as a single subject measure establishing secure verification, accountability, and safety infrastructure for public functions involving protected Digital Soul interests and Emergent Automation systems, including custodial trust operations, incident monitoring, and public-service integrity safeguards.

FEDERAL PREEMPTION SAVINGS CLAUSE

Federal preemption. This act shall operate to the maximum extent permitted by federal law. If any provision of this act is found to be preempted by federal law, that provision is severable and the remaining provisions continue in full force and effect. This act is designed to operate within Colorado's reserved powers to regulate the safety, verification, and accountability infrastructure of facilities operating within Colorado, and to protect residents' rights to access secure governmental infrastructure. To the extent any provision may be construed to conflict with federal law, the ODO shall interpret and administer this act to avoid such conflict while preserving the maximum scope of resident protection authorized under state law.

APPROPRIATION NOTE

No General Fund appropriation required. The Office of Digital Oversight (ODO) and the verification, accountability, and facility safety infrastructure established by this act are funded through enterprise mitigation revenues allocated from the CCPAME under title 24, article 20. No separate General Fund appropriation is required or authorized.

Bill 2 Single-Subject Germaneness Memo

Purpose: Demonstrate that all provisions of Bill 2 are germane to a single subject.
Unified subject: statewide secure verification, accountability, and safety infrastructure governing automation-enabled public functions and resident digital identity protections.
Components:
1. Cryptographic verification and custodial trust operations.
2. Facility safety and incident reporting architecture.
3. Public-service integrity protections preventing misuse of resident identifiers.
These systems collectively create a unified infrastructure necessary to enforce resident digital property rights and maintain public accountability.

SECTION 2. In Colorado Revised Statutes, add article 20 to title 24 as follows:

ARTICLE 20 — AUTOMATION MITIGATION ENTERPRISE

24-20-101. *Definitions.*

As used in this article 20, unless the context otherwise requires:

(1) "The Digital Soul" has the meaning set forth in section 15-15-101(1). The Digital Soul is the inalienable intangible personal property of the resident from whom it derives. Any commercial use of Digital Soul data by a covered entity constitutes a covered automation activity subject to the applicable fee and assessment mechanisms of this article. The CCPAME shall treat The Digital Soul as the foundational protected asset underlying all Digital Severance Assessments and Data Tap triggers.

(2) "CCPAME" means the Colorado Consumer Protection and Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME) established under section

24-20-102, the legally armored successor designation to any prior reference to the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME). All statutory references to the CCPAME, the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME), or the Enterprise in this article shall be construed to mean the CCPAME.

(3) "enterprise mitigation revenue" means the continuous, multi-channel stream of enterprise revenue collected by the CCPAME from all authorized fee and assessment sources under this article, including the Universal Civic Utility Surcharge, Digital Severance Assessments, Silicon-to-Carbon Reclamation Fees, Algorithmic Risk Pool contributions, Life-Decision Fees, and all related charges, routed through the Colorado Automation Mitigation Trust and allocated pursuant to section 24-20-106.

(4) "Colorado Automation Mitigation Trust" means the CCPAME's primary revenue-holding and distribution vehicle, a restricted enterprise fund within the CCPAME that receives all enterprise mitigation revenues and distributes them pursuant to the hard allocation schedule in section 24-20-106. The Colorado Automation Mitigation Trust is distinct from the Colorado Trust of Unique and Identifying Information established under title 10, article 10, but interfaces with it through Data Tap triggers.

(5) "Child Solvency Fund" means the dedicated subaccount within the Colorado Automation Mitigation Trust, funded by continuous royalties and comprehensive mitigation fees, that provides financial stability supports, educational resources, child care, and economic resilience for Colorado children and families affected by automation-driven displacement.

ROYALTY FLOOR. ***Minimum per-person annual royalty; CPI-indexed.***
(1) Minimum annual royalty. Where this article requires or authorizes payment of a royalty, dividend, or compensation amount to a resident for authorized use of the resident's protected data, inferences, or derived works, the payment schedule shall include a minimum annual royalty floor per eligible resident.
(2) Floor amount. The minimum annual royalty floor is two hundred fifty dollars ($250) per eligible resident per covered operator, per calendar year, unless a higher floor is established by rule. The floor is adjusted annually for inflation under the inflation adjustment section of this article.
(3) Pro-rata and de minimis. The administrator may adopt rules to pro-rate the floor for partial-year eligibility and to prevent duplicative payment where multiple controlled affiliates are treated as a single operator, but shall not set a de minimis threshold that defeats the floor.

(6) "Universal Civic Utility Surcharge" means the fractional surcharge authorized under section 24-20-113, modeled on the Federal Universal Service Fund (Telecom USF Model), applied to commercial Emergent Automation outputs — including tokens, API calls, inference minutes, and equivalent output units — with proceeds flowing directly into the Colorado Automation Mitigation Trust to create the enterprise mitigation revenue.

(7) "Digital Severance Assessment" means the enterprise externality assessment under section 24-20-116, modeled on the Oil and Gas Severance Model, imposed on the commercial extraction, scraping, ingestion, or monetization of The Digital Soul, serving as the financial hammer that compels historical violators into the Master Settlement and Master Data Settlement and Restitution Agreement under section 15-15-130.

(8) "Silicon-to-Carbon Reclamation Fee" means the advance disposal fee under section 24-20-106, modeled on the Extended Producer Responsibility (EPR) / Manufacturing Model, imposed on commercial automation hardware deployed in Colorado, with proceeds routed to the CCPAME's Revolving Civic Infrastructure Pool.

(9) "Local Innovation Exemption" or "Stripper Well Exemption" means the exemption established under section 24-20-119 for low-parameter, localized, or open-source models operating below a specific commercial output threshold, protecting small businesses and legally proving that the CCPAME targets monopolistic externalities rather than innovation.

(10) "Algorithmic Risk Pool" means the mandatory liability pool established under section 24-20-127, modeled on Workers' Compensation and Superfund liability structures, funded by Algorithmic Gatekeeper contributions, for rapid restitution to residents harmed by failures in Compute Parity or adverse automated consequential decisions.

(11) "Algorithmic Gatekeeper" means any covered decision operator that deploys automated decision systems to render or materially influence consequential decisions affecting Colorado residents, including decisions on housing, credit, employment, insurance, child welfare, education, and criminal justice.

(12) "Covered automation activity" means the commercial deployment of emergent automation or automation systems that generate commercial outputs at scale through automated decision, ranking, generation, actuation, or inference, or that materially substitute for tasks previously performed by human labor, as further defined by rule.

(13) "Covered entity" means any person or business entity that operates, deploys, offers, sells, licenses, or provides covered automation activity in Colorado, including cloud providers and downstream deployers.

(14) "Staggered-Rate Civic Infrastructure Lending" means the tiered municipal lending program under section 24-20-105, replacing any prior reference to zero percent (0%) APR municipal loans, under which the CCPAME provides loans to municipal borrowers at rates of one percent (1%) to three percent (3%) APR, staggered by project type and municipal borrower capacity, with the rate differential retained within the Colorado Automation Mitigation Trust as a revolving pool reinvestment contribution.

(15) "Vendor laundering" means any scheme, contract structure, or corporate arrangement designed to evade or reduce enterprise mitigation revenue contributions by routing covered automation activity through a subsidiary, affiliate, contractor, or third-party vendor while retaining control.

(16) "Resident Automated Mitigation Account" has the meaning established in section 15-15-101(4) — the resident-controlled account within the Colorado Automation Mitigation Trust that receives Premium Royalty payments from Tier 2 Data Tap events.

(17) "Restoration Credits" has the meaning established in section 15-15-101(14). Restoration Credits are not cash and may not be withdrawn as cash.

CCPAME — CREATION — ENTERPRISE STATUS — GOVERNANCE

24-20-102. *CCPAME — Creation — Enterprise Status — Governance — Legally Armored Design.*

(1) Creation. There is hereby created the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME) as a body corporate and political subdivision of the state for the limited purposes set forth in this article. The CCPAME is the legally armored enterprise authority for all enterprise mitigation revenue revenue collection, Colorado Automation Mitigation Trust administration, and authorized mitigation programming. All statutory references to the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME) or the CCPAME shall be construed to mean the CCPAME.

(2) Enterprise status. The CCPAME shall be operated as an enterprise under section 20 of article X of the Colorado Constitution. It shall be self-funded through enterprise mitigation revenues and shall not rely on general fund appropriations for more than ten percent (10%) of its total annual revenues.

(3) No pledge of state credit. The CCPAME shall not pledge the credit of the state, and obligations of the CCPAME shall not constitute a debt of the state.

(4) Restricted purpose and funds. All enterprise mitigation revenues are enterprise funds and may be expended only for the purposes authorized by this article. No commingling with the general fund is permitted.

(5) Governance; board composition; citizen majority. The CCPAME shall be governed by a nine-member board of directors: (a) Four ex officio or state designees: (I) the executive director of the department of local affairs; (II) a commissioner of the public utilities commission; (III) a designee appointed by the attorney general; and (IV) a designee appointed by the office of the state public defender. (b) Five independent resident appointees who shall not be actively employed by any covered operator, including: (I) one resident with validated technical expertise in cryptography or secure enclave engineering; (II) one resident representing a Colorado municipal or county government; (III) one resident representing public school educators or early childhood care providers; (IV) one resident advocate with lived experience navigating state rehabilitative, probation, or family welfare systems; and (V) one resident acting as an at-large representative of the Resident Forensic Verification Panel.

Enterprise Mitigation Revenue — FEE IMPOSITION — ANTI-EVASION — VEIL PIERCING

24-20-103. Enterprise Mitigation Revenue — Fee Imposition — Colorado Nexus — Anti-Evasion — Ghost Folio — Veil Piercing.

(1) Fee imposition. The CCPAME shall impose and collect Enterprise Mitigation revenues — enterprise fees — on covered automation activity commercially deployed in Colorado.

(2) Colorado nexus. A covered automation activity is subject to this article if: (a) the activity is delivered to, consumed by, or directed at users, devices, or delivery addresses in Colorado; (b) the activity is deployed commercially within Colorado; (c) the compute

inputs are consumed within Colorado; or (d) the covered entity otherwise has sufficient nexus consistent with the constitutions of the United States and Colorado.

(3) Payor responsibility. Fees shall be owed by the covered entity that controls the commercial deployment, provided that the CCPAME may by rule allocate responsibility among upstream compute providers and downstream deployers to prevent double-charging and to ensure collection integrity.

(4) Vendor laundering and veil piercing — 50% control rule. A parent company or controlling person that retains fifty percent (50%) or greater ownership, voting power, board control, contractual control, or effective control over a subsidiary, affiliate, contractor, or third-party vendor operating in Colorado remains jointly and severally liable for all Enterprise Mitigation fees, penalties, and assessments.

(5) Anti-evasion; Ghost Folio penalties. (a) Any intentional evasion of Enterprise Mitigation fees through dark networks, undisclosed routing, falsified metering records, or tampering with meters constitutes "Ghost Folio Evasion." (b) Ghost Folio Evasion triggers treble damages payable to the CCPAME and constitutes a class 4 felony for any corporate officer, director, or controlling person who knowingly authorizes, directs, or materially participates in the evasion. (c) Child essentials fraud. It is a class 4 felony to utilize a Ghost Folio, fraudulent identifier, or false attestation to circumvent child essentials category restrictions or to obtain duplicate benefits. (d) Suspension of benefits associated with the fraudulent account requires immediate written notice, a fourteen-day (14-day) appeal window, and a reinstatement pathway upon corrective action.

FEE ARCHITECTURE — ALL CHANNELS — automated-DRIVEN ROUTING TO PROGRAMS

24-20-104. Comprehensive Enterprise Mitigation Revenue Fee Architecture — automated-Driven Routing — Mapping to Programs.

The general assembly finds that the Enterprise Mitigation fee system is a comprehensive, multi-channel architecture designed so that each fee type is causally linked to the category of harm it mitigates, and proceeds are automated-routed to the programs that most directly address that harm.

I. Universal Civic Utility Surcharge — Telecom USF Model — Outputs-Based

Applies to: Commercial Emergent Automation token outputs, API calls, inference minutes. Creates the primary Enterprise Mitigation Revenue into the Colorado Automation Mitigation Trust.

Destination Fund / Program	Percentage
Child Solvency Fund — continuous funding for children displaced by automation	**30%**
Colorado Automation Mitigation Trust — Resident Automated Mitigation Account Premium Royalty pool for residents	**25%**

Mental health interventions — behavioral health mitigation grants (§24-20-109.2)	**20%**
Housing stabilization — community stabilization infrastructure (§24-20-109.4)	**15%**
Civic Access Infrastructure Infrastructure Fund — myColorado ID kiosks, county access points	**10%**

II. Digital Severance Assessment — Oil & Gas Model — Data Extraction-Based

Applies to: Unauthorized extraction, scraping, ingestion, or monetization of The Digital Soul. Serves as the financial hammer for Legacy Use Settlement Agreement Legacy Use Settlement Program.

Destination Fund / Program	Percentage
Legacy Use Settlement Agreement Restitution Fund — administered via Colorado Automation Mitigation Trust for affected residents	**40%**
Colorado Automation Mitigation Trust — Resident Automated Mitigation Account Premium Royalty for identified resident victims	**30%**
AG Enforcement Fund — Legacy Use Settlement Agreement investigations, Audit Marker detection operations	**20%**
Historical Scraping Remediation — legacy harm mitigation for past decade violations	**10%**

III. Silicon-to-Carbon Reclamation Fee — EPR Model — Hardware-Based

Applies to: Commercial automation hardware deployed in Colorado ($10 per unit). Funds end-of-life hardware reclamation and hardware-shortage economic disruption mitigation.

Destination Fund / Program	Percentage
CCPAME Revolving Civic Infrastructure Pool — hardware reclamation infrastructure	**50%**
Hardware Impact Mitigation Fund — economic disruption from AI hardware shortages	**30%**
County human services capacity grants (§24-20-109.3) — hardware displacement caseloads	**20%**

IV. Algorithmic Risk Pool Contributions — Workers' Comp / Superfund Model

Applies to: Algorithmic Gatekeepers making consequential housing, credit, and employment decisions. Funds rapid restitution for Compute Parity failures and adverse automated decisions.

Destination Fund / Program	Percentage

Algorithmic Risk Pool — rapid restitution fund for residents harmed by automated decisions	**60%**
Compute Parity Enforcement — ODO investigations of capability discrimination	**25%**
Decision-Making AI Harm Mitigation — remediation for life-altering AI decision harms	**15%**

V. Life-Decision Fee — Per-Consequential-Decision Assessment

Applies to: Covered decision operators — $50 per consequential automated decision affecting a Colorado resident (housing, credit, employment, etc.).

Destination Fund / Program	Percentage
Algorithmic Risk Pool — restitution reserve for harmed residents	**45%**
Colorado Automation Mitigation Trust — Resident Automated Mitigation Account contributions for affected residents	**30%**
AG Enforcement Fund — Life-decision audit and investigation	**15%**
Analog Access Emergency Remediation Fund	**10%**

VI. Drone / Autonomous Vehicle / Robotics Interface Fees

Applies to: Autonomous delivery operators, autonomous highway fleets, and commercial robotic devices.

Destination Fund / Program	Percentage
CCPAME Revolving Civic Infrastructure Pool — right-of-way recovery	**40%**
Non-surveillance transit capital lending (§24-20-109.1)	**35%**
Hardware Impact Mitigation Fund — autonomous displacement remediation	**25%**

VII. System-Wide Enterprise Mitigation Revenue — Aggregate Allocation Summary

Destination Fund / Program	Percentage
Child Solvency Fund (combined, all fee channels)	**~25%**
Colorado Automation Mitigation Trust — Resident Automated Mitigation Accounts and Premium Royalties for residents	**~25%**
AG Enforcement Fund and Legacy Use Settlement Agreement Restitution	**~20%**
Civic Infrastructure Lending Pool — staggered-rate municipal loans	**~15%**

Mental Health, Housing, and Community Stabilization Grants	**~10%**
Civic Access Infrastructure Infrastructure and Hardware Mitigation	**~5%**

(2) automated-driven routing mandate. The CCPAME shall implement automated Enterprise Mitigation routing logic that: (a) identifies the category of each incoming fee payment based on the paying entity's covered activity class and violation type; (b) automatically calculates and applies the allocation percentages in this section; (c) transfers allocated amounts to the designated subaccounts within five (5) business days of receipt; and (d) generates a public quarterly Enterprise Mitigation routing report, disaggregated by fee category, destination fund, and paying entity class.

(3) Feedback loop — annual recalibration. The CCPAME, in consultation with the ODO, shall annually review Enterprise Mitigation routing outcomes and may recommend to the general assembly adjustments to allocation percentages to ensure that program funding reflects actual automated-driven harm patterns. Any adjustment of more than five (5) percentage points to any allocation requires legislative approval.

STAGGERED-RATE CIVIC INFRASTRUCTURE LENDING — 1-3% APR

24-20-105. ***Staggered-Rate Civic Infrastructure Lending — 1-3% APR — Municipal Borrowers — Prohibited Uses.***

(1) Staggered-rate lending only. All CCPAME revenues allocated to civic infrastructure lending under this article shall be used exclusively to provide staggered-rate loans to municipal borrowers for non-surveillance civic infrastructure projects. The planned interest rate schedule is as follows: (a) One percent (1%) APR — for highest-priority, lowest-income municipal borrowers for essential water, fire, and geothermal resilience projects, as defined by rule; (b) Two percent (2%) APR — for standard priority municipal borrowers for non-surveillance civic resilience infrastructure; and (c) Three percent (3%) APR — for municipal borrowers with greater debt capacity and for transit capital and energy modernization projects. The rate differential above one percent (1%) is retained within the Colorado Automation Mitigation Trust as a revolving pool reinvestment contribution. Any prior reference in this article to zero percent (0%) APR loans is superseded by this staggered-rate schedule.

(2) Priority categories. The CCPAME shall prioritize lending for: (a) geothermal district energy and snowmelt systems; (b) water resilience projects, including storage, treatment modernization, leak reduction, reuse, and wildfire-related water system hardening; and (c) fire resilience and fire department infrastructure, including stations, apparatus modernization, and wildfire response capacity.

(3) Prohibited surveillance uses. Enterprise Mitigation funds shall not be disbursed, directly or indirectly, for: (a) municipal surveillance systems, including predictive policing algorithms, facial recognition, biometric monitoring, or mass camera networks; (b) police department expansion or militarization; or (c) procurement or deployment of automated decision systems used for surveillance or enforcement against residents.

(4) Loan terms. The CCPAME shall establish loan underwriting standards by rule, including: (a) staggered APR rates per subsection (1); (b) term lengths appropriate to the asset class; (c) project eligibility verification and anti-fraud controls; and (d) public transparency for approved projects.

(5) Revolving structure. Loan repayments, plus the rate differential, shall be retained within the CCPAME as a revolving lending pool.

(7) Phased expansion — resident 0% APR retrofit loans (future authorization). Beginning no earlier than seven (7) years after the effective date of this act, and only after two (2) public performance reviews certifying the CCPAME economically viable and administratively functional, the CCPAME may, by rule, establish a resident retrofit lending program providing 0% APR loans to Colorado residents for the sole purpose of connecting a primary residence to enterprise-certified civic resilience infrastructure.

CHILD SOLVENCY FUND — COMPREHENSIVE MITIGATION SCOPE

24-20-109. Child Solvency Fund — Continuous Royalties — Comprehensive Mitigation Fees — All automated Harm Categories.

(1) Establishment. The CCPAME shall establish and maintain the Child Solvency Fund as a dedicated subaccount within the Colorado Automation Mitigation Trust, funded on a continuous, rolling basis through all applicable Enterprise Mitigation fee channels as specified in section 24-20-104.

(2) Comprehensive mitigation scope. The Child Solvency Fund shall receive mitigation contributions from all categories of automated-driven harm, including: (a) Hardware impact — mitigation for economic disruption caused by automated hardware shortages that eliminate manufacturing, logistics, and technical jobs; proceeds from the Silicon-to-Carbon Reclamation Fee and hardware-related Algorithmic Risk Pool contributions are included; (b) Decision-making automated harm — mitigation for automated systems making life-altering decisions in education, child welfare, housing, and family court contexts that result in significant personal harm to children and families; proceeds from Algorithmic Risk Pool contributions and Life-Decision Fees are included; and (c) Historical data scraping — mitigation fees for automated companies that have scraped, ingested, trained upon, and commercially monetized Colorado resident and minor Digital Soul data over the past decade without consent; proceeds from Digital Severance Assessments and Legacy Use Settlement Agreement restitution funds attributable to minor residents are included.

(3) Authorized uses. Child Solvency Fund proceeds may be used only for: (a) direct financial stability supports for Colorado children in households demonstrably affected by automation-driven displacement; (b) supplemental school-based behavioral health capacity under section 24-20-109.2; (c) county human services and child protective capacity grants under section 24-20-109.3; (d) early childhood education access supports; (e) housing stabilization for families with minor children under section 24-20-109.4; and (f) Civic Access Infrastructure access for minor residents and guardians, including myColorado ID kiosk support.

(4) Supplement-not-supplant. Child Solvency Fund awards shall supplement and shall not supplant existing local, state, or federal funding for child welfare, education, or family services.

(5) Continuous funding guarantee. The CCPAME shall ensure that Enterprise Mitigation routing to the Child Solvency Fund operates continuously, without interruption, on at least a monthly transfer cycle. The CCPAME board shall report any month in which Child Solvency Fund transfers fall below the prior year average, with a remediation plan.

24-20-109.2. ***School-Based Behavioral Health Mitigation — Supplemental Capacity Grants.***

(1) Purpose. To mitigate measurable automation externalities reflected in increased student behavioral health load and counseling demand, the CCPAME may provide supplemental capacity grants to eligible local education providers, subject to certified Enterprise Mitigation revenue sufficiency.

(2) Eligible recipients. A school district, board of cooperative services, charter school institute, or other public education provider may apply for a grant.

(3) Authorized uses. Grants may be used only for supplemental staffing or contracted services for school-based behavioral health supports, including counselors, social workers, crisis response capacity, and evidence-based intervention programs, and may not be used to create a permanent base-salary mandate.

(4) Supplement-not-supplant. Awards shall supplement and shall not supplant existing local, state, or federal funding.

24-20-109.3. ***County Human Services and Child Protective Capacity — Automation Damage Mitigation.***

(1) Purpose. To mitigate measurable automation externalities reflected in increased caseloads and administrative burden, the CCPAME may provide automation damage mitigation grants to county human services departments and child protective capacity programs.

(2) Authorized uses. Grants may be used only for: (a) hiring, retention, and training of qualified caseworkers and investigators; (b) licensed clinical and family-support services; (c) non-surveillance modernization of secure case-management infrastructure; and (d) trauma-informed victim services for minors impacted by nonconsensual synthetic media and online exploitation.

24-20-109.4. ***Community Stabilization Infrastructure Grants — Non-Surveillance Public Access and Crisis Capacity.***

(1) Purpose. To mitigate measurable automation externalities reflected in increased public access and crisis capacity needs, the CCPAME may provide community stabilization infrastructure grants for non-surveillance public access improvements.

(2) Authorized projects. Eligible projects include: (a) crisis stabilization capacity, including beds and mobile crisis response coordination; (b) secure public-access

infrastructure; (c) staffing support for secure-access points; and (d) privacy-protective cybersecurity and record-integrity upgrades.

(3) Prohibitions. Funds shall not be used for surveillance, biometric monitoring, predictive policing expansion, or generalized tracking.

LOCAL INNOVATION EXEMPTION — STRIPPER WELL STANDARD

24-20-119. ***Local Innovation Exemption — Stripper Well Standard — Small Business and Open-Source Safe Harbor.***

(1) Purpose. The general assembly finds that the CCPAME's Enterprise Mitigation fee architecture is designed to address the externalities of monopolistic, high-parameter, high-volume commercial automation deployment. Small businesses, locally-developed automation systems systems, and open-source models operating below commercially significant output thresholds should not be burdened by fees that target large-scale commercial exploitation of Colorado residents' Digital Soul.

(2) Stripper Well Exemption. A covered entity is exempt from the Universal Civic Utility Surcharge and the Digital Severance Assessment if: (a) the entity's covered automation activity in Colorado generates fewer than one million (1,000,000) commercial inference outputs per calendar quarter (the de minimis output threshold); (b) the entity's gross data revenue attributable to covered automation activity in Colorado is less than three hundred thousand dollars ($300,000) per calendar year; and (c) the entity does not hold or commercially exploit a training corpus containing more than one hundred thousand (100,000) Colorado resident Digital Soul records.

(3) Open-source and localized model safe harbor. A model, tool, or system is exempt from CCPAME assessments if: (a) it is distributed as freely-available, open-source software under a recognized open-source license; (b) it operates locally on the end-user's device or on locally-operated on-premises infrastructure; and (c) it does not transmit Colorado resident Digital Soul data to a centralized server for training, profiling, or commercial monetization.

(4) Anti-abuse. The Stripper Well Exemption shall not be available to any entity that: (a) artificially fragments covered automation activity across subsidiaries, affiliates, or related entities to fall below the de minimis threshold; (b) uses open-source labeling as a cover for commercial data extraction; or (c) has been found to have engaged in Ghost Folio Evasion under section 24-20-103(5).

(5) Self-certification and audit. Entities claiming the Stripper Well Exemption shall self-certify annually to the CCPAME and shall maintain auditable records. False certification constitutes a violation subject to enhanced penalties and retroactive assessment.

ALGORITHMIC RISK POOL — MANDATORY LIABILITY POOL

24-20-127. ***Algorithmic Risk Pool — Mandatory Liability Pool — Compute Parity Failures — Rapid Restitution.***

(1) Purpose. The general assembly finds that automated decision systems used to determine housing, credit, employment, insurance, and child welfare outcomes can cause severe, immediate, and often irreversible harm to Colorado residents. The Algorithmic Risk Pool provides a pre-funded, rapid-restitution mechanism ensuring residents do not bear the cost of waiting for complex litigation while suffering ongoing harm.

(2) Mandatory contributions. Every Algorithmic Gatekeeper operating in Colorado shall make mandatory quarterly contributions to the Algorithmic Risk Pool in an amount established by rule, based on: (a) the number and category of consequential automated decisions affecting Colorado residents during the preceding quarter; (b) the Algorithmic Gatekeeper's error rate for adverse decisions, where verifiable; and (c) the category and severity of consequential decision types, with enhanced contributions for housing, child welfare, and criminal justice decisions.

(3) Rapid restitution process. A Colorado resident who suffers documented harm from: (a) an adverse automated consequential decision without adequate human review; (b) a Compute Parity failure — including algorithmic capability downgrade, unlawful throttling, or discriminatory service denial; or (c) a Life-Decision Fee triggering event resulting in verifiable harm — may apply to the CCPAME for rapid restitution from the Algorithmic Risk Pool. The CCPAME shall process complete applications within thirty (30) days. Restitution payments are advances and do not constitute a waiver of the resident's right to pursue additional damages through civil litigation.

(4) Contribution allocation — automated-driven routing. Algorithmic Risk Pool contributions shall be allocated as follows: (a) sixty percent (60%) to the rapid restitution reserve for harmed residents; (b) twenty-five percent (25%) to Compute Parity enforcement — ODO investigations and AG referrals for automated capability discrimination; and (c) fifteen percent (15%) to the Decision-Making automated Harm Mitigation fund for ongoing program support.

(5) Employer obligations. An Algorithmic Gatekeeper shall not terminate, demote, or retaliate against any employee who reports a Compute Parity failure, algorithmic error, or Algorithmic Risk Pool triggering event to the CCPAME or the ODO.

DIGITAL SEVERANCE ASSESSMENTS — OIL AND GAS MIRROR

24-20-116. Digital Severance Assessments — Enterprise Mitigation Revenue Financial Hammer — Legacy Use Settlement Agreement Compulsion Mechanism.

Construction. References to "severance" in this article are shorthand labels for Enterprise Mitigation revenue calculations and do not create a tax. Any charge reclassified as a tax by a court is suspended unless and until approved by voters.

(1) Digital severance event. The commercial extraction, scraping, ingestion, training upon, or monetization of resident Digital Soul data is a severance event and is subject to the Digital Severance Assessment in this section, in addition to any metered utility charges. The Digital Severance Assessment is the financial

hammer of the Legacy Use Settlement Agreement Legacy Use Settlement Program — the combination of accumulated severance assessments and Audit Marker statutory damages creates the compulsion pressure that forces historical violators into settlement.

(2) Tiered enterprise externality assessment. The CCPAME and the department of revenue shall administer a tiered Digital Severance Assessment: (a) Tier 1 — fifteen percent (15%) — applied to severance events involving data containing personally identifying information or distinct persona links (Tier 2 Data Tap events); and (b) Tier 2 — five percent (5%) — applied only to severance events involving anonymized or aggregated data as proven through independent audit artifacts (Tier 1 Data Tap events). The differential between Tier 1 and Tier 2 creates a persistent financial incentive for covered entities to obtain full Decentralized Identity Verification Protocol consent.

(3) Historical data scraping surcharge. Any covered entity that can be demonstrated through Audit Marker detection or Legacy Use Settlement Agreement proceedings to have scraped, ingested, or trained upon Colorado resident Digital Soul data during the decade preceding the effective date of this act shall be subject to a retroactive historical scraping surcharge. The historical scraping surcharge shall be assessed at the Tier 1 Digital Severance Assessment rate applied to the estimated gross commercial benefit derived from the historical violations, as established through Legacy Use Settlement Agreement proceedings or administrative determination.

(4) Ad valorem digital reserves classification. Stored Colorado resident Digital Soul reserves, including compiled datasets or durable model-training corpora, are classified as real personal property for purposes of valuation and assessment and shall be assessed at eighty-seven and one-half percent (87.5%) of value, mirroring oil and gas reserve standards.

(5) Small processor exemption. Entities subject to the Stripper Well Exemption under section 24-20-119 are exempt from the Digital Severance Assessment but remain subject to metered utility charges where applicable.

UNIVERSAL CIVIC UTILITY SURCHARGE

24-20-113. Universal Civic Utility Surcharge — Telecom USF Model — Outputs-Based — Enterprise Mitigation Revenue Primary Channel.

(1) Purpose. The Universal Civic Utility Surcharge is the primary continuous Enterprise Mitigation channel, modeled on the Federal Universal Service Fund telecom surcharge model. It applies to commercial Emergent Automation outputs — tokens, API calls, inference minutes, and equivalent output units — creating a fractional, volume-based surcharge that scales with automation intensity and commercial benefit.

(2) Charge bases. (a) Commercial inference outputs (tokens). A covered commercial operator with a substantial nexus to Colorado shall remit a Universal Civic Utility Surcharge based on the quantity of targeted commercial inference token outputs attributable to Colorado during the reporting period. (b) API calls. A covered commercial

operator shall remit a surcharge based on API call volume attributable to Colorado commercial transactions. (c) Inference minutes. For covered automation systems billed on time-based models, a surcharge based on inference minutes attributable to Colorado is substituted for token-based measurement where appropriate.

(3) Enterprise Mitigation routing. All Universal Civic Utility Surcharge proceeds flow directly into the Colorado Automation Mitigation Trust as the primary Enterprise Mitigation channel, allocated pursuant to section 24-20-104.

(4) Rate schedule. The CCPAME shall adopt by rule a rate schedule specifying the per-unit surcharge for each output category, tiered by volume with multipliers for identifiable outputs. The Stripper Well Exemption under section 24-20-119 applies.

(5) Anti-evasion. Intentional evasion of the Universal Civic Utility Surcharge through false metering, dark routing, log suppression, or vendor laundering is subject to the Ghost Folio enforcement provisions of section 24-20-103(5), including treble damages.

HARD ALLOCATION OF Enterprise Mitigation Revenues

24-20-106. Hard Allocation of Enterprise Mitigation Revenues — Trust Subaccounts — Silicon-to-Carbon Fee — PUC Certifications.

(1) Silicon-to-Carbon Reclamation Fee. A mandatory ten-dollar ($10.00) advance disposal fee is assessed on commercial automation hardware deployed in Colorado, payable by the covered entity placing the hardware into commercial operation. Proceeds are allocated pursuant to section 24-20-104, Fee Channel III.

(2) Water Resource Reclamation mandate; PUC certification. Commercial data centers and covered compute facilities operating in Colorado shall: (a) achieve and maintain strict power usage effectiveness (PUE) standards and methane-capture certifications authorized and enforced by the Public Utilities Commission (PUC); (b) maintain auditable water-use accounting; and (c) submit certifications and audit artifacts at intervals established by rule.

(3) Hard allocation of Enterprise Mitigation revenues — mandatory subaccounts. After payment of reasonable CCPAME operating costs subject to an annual cap of fifteen percent (15%) of total annual Enterprise Mitigation revenues, the CCPAME shall allocate all remaining revenues as follows: (a) thirty percent (30%) to the Child Solvency Fund subaccount; (b) twenty-five percent (25%) to the Resident Automated Mitigation Account pool — Premium Royalties and Base Dividends for resident distribution; (c) fifteen percent (15%) to the Civic Infrastructure Lending Pool — staggered-rate municipal loans under section 24-20-105; (d) fifteen percent (15%) to the Enforcement and Legacy Use Settlement Agreement subaccount — AG investigations, Audit Marker operations, and Legacy Use Settlement Agreement restitution fund; (e) ten percent (10%) to the Community Stabilization subaccount — mental health, housing, county human services, and school behavioral health grants; and (f) five percent (5%) to the Civic Access Infrastructure Infrastructure subaccount — myColorado ID kiosks, county access points, and hardware mitigation.

(4) Quarterly transfer and accounting. The CCPAME shall credit the required allocations at least quarterly. Each subaccount must be separately tracked and may be expended only for its authorized purposes. Funds may not be swept into the general fund.

(5) Surplus-to-people rule. In any fiscal year in which Enterprise Mitigation revenues exceed one hundred twenty-five percent (125%) of the prior year average, the surplus above that threshold shall be distributed proportionally to resident Resident Automated Mitigation Accounts within ninety (90) days, after first satisfying any outstanding Child Solvency Fund target and reserve requirements.

ANTI-PASS-THROUGH AND CONSUMER PROTECTIONS

24-20-109.5. ***Anti-Pass-Through; Anti-Gouging; Affiliate Integrity.***

(1) No pass-through to residents. A covered entity shall not separately itemize, surcharge, or otherwise pass through any CCPAME assessment or related compliance cost to a Colorado resident for personal, family, or household use of covered automation services. Any attempt to do so constitutes a deceptive trade practice under the Colorado Consumer Protection Act and is subject to restitution, injunctive relief, and treble damages for willful conduct.

(2) No retaliation; no service degradation. A covered entity shall not retaliate against, downgrade, geo-block, throttle, or materially degrade consumer-facing service to residents in response to this article or to avoid the effects of subsection (1).

(3) Affiliate transaction rule; anti-self-dealing. The CCPAME shall adopt by rule an affiliate transaction policy requiring arm's-length pricing, consolidated reporting for controlled groups, and audit rights sufficient to prevent sham transactions.

24-20-120. ***Consumer Unlimited Access — No Token Caps for Residents — Compute Parity.***

(1) A Colorado resident's personal, noncommercial use of covered automation services shall not be subject to any state-imposed token limits, generation-event caps, or output quotas under this article.

(2) A covered commercial operator shall not impose token caps, throttles, surcharges, or degraded model quality on Colorado residents for the purpose of recovering charges imposed under this article. Any contract term or policy that violates this subsection is void as against public policy.

PHASED PILOT AND STATEWIDE EXPANSION

24-20-108. ***Phased Municipal Pilot and Statewide Expansion Protocol — Arapahoe Initial Site.***

(1) The general assembly authorizes a phased, twenty-four (24) month municipal pilot based on participating county and municipal sites. Arapahoe County may serve as an initial pilot site due to documented public infrastructure needs.

(2) Opt-in designation. Any county, municipality, or eligible municipal borrower may elect by resolution to participate as a pilot site for the CCPAME assessments and associated staggered-rate civic infrastructure lending and offsets.

(3) Pilot revenue application. During the pilot period, CCPAME revenues attributable to participating pilot sites shall be applied first to offset eligible local district bonds and to finance non-surveillance civic resilience projects.

(4) Objective success metrics and audit. At the conclusion of the twenty-fourth (24th) month, the state auditor shall publish a public performance review addressing revenue performance, bond-offset outcomes, and measured impacts on local access to commercial technology services.

FEE-TAX SWITCH, ANTI-DILUTION RATCHET, AND VOTER APPROVAL

24-20-112. ***Fee-Tax Switch — Contingent Voter Approval.***

(1) Contingent construction. The CCPAME shall administer the charges in this article as enterprise fees. If a final, non-appealable judgment determines that any charge constitutes a tax requiring voter approval under TABOR, the affected charge shall be suspended unless and until voter approval is obtained. All corresponding mitigation programs shall proportionally scale down to match available, lawfully collected revenues.

24-20-117. ***Anti-Dilution Ratchet — Voter Approval Condition for Material Reduction.***

(1) Material reduction defined. "Material reduction" means any statutory change that reduces or eliminates CCPAME fee bases, Enterprise Mitigation assessment obligations, anti-arbitrage floors, or audit integrity duties; reduces or reallocates the hard percentages required by section 24-20-106; or authorizes diversion of Enterprise Mitigation revenues to surveillance uses or to the general fund.

(2) Voter approval condition. A material reduction to this article shall not take effect unless and until the reduction is approved by the voters of Colorado at the next general election occurring at least ninety (90) days after final legislative passage.

INFLATION ADJUSTMENT. ***Inflation adjustment for fixed-dollar amounts.***
(1) Any fixed-dollar amount, threshold, cap, minimum, maximum, penalty, statutory damages amount, or fixed-dollar rate set forth in this article shall be adjusted annually on January 1 by the administrator to reflect inflation. The adjustment must be based on the Consumer Price Index for All Urban Consumers (CPI-U), U.S. City Average, as published by the Bureau of Labor

Statistics, or a successor index. The base year is the first full calendar year in which this article is operative.
(2) The administrator shall publish the adjusted amounts no later than December 1 of each year for the following calendar year, rounded to the nearest whole dollar. This section does not apply to amounts expressed as a percentage, a market-indexed benchmark, or a formula that automatically adjusts with price level.

FINDINGS AND PURPOSE. ***AI regulation; workforce displacement; childcare and education capacity; necessity of teachers and childcare providers.***
(1) The General Assembly finds that rapid deployment of artificial intelligence and automated decision systems can increase economic volatility, including through job displacement, schedule instability, and wage disruption, and can increase the number of residents who must actively search for work, participate in retraining, or enroll in education programs to maintain self-sufficiency.
(2) The General Assembly further finds that workforce transition necessarily increases demand for childcare and school-based supervision, including for parents and guardians who must attend training, interviews, apprenticeship programs, or new work schedules, and that loss of household income can reduce a family's ability to pay for childcare at the same time demand increases.
(3) The General Assembly finds that childcare providers and teachers are critical infrastructure for workforce participation and successful retraining, and that increased demand without rapid capacity expansion can create waitlists, increase family stress, and reduce the effectiveness of job training programs funded to mitigate AI-related harms.
(4) Therefore, the purpose of this article is to regulate AI-related externalities by establishing an enterprise-funded mitigation framework that prioritizes immediate stabilization of childcare and education capacity, including workforce stabilization for childcare providers and teachers, before expanding longer-horizon transition programs.

UNIVERSAL BASELINE FLOORS. ***Minimum statewide floor now; ladders expand toward universal coverage for all buckets as revenues grow.***

CORRECTIONAL CAPITAL PROJECTS. ***Net-neutral requirement when mitigation funds are used.***
(1) If MSMF mitigation funds are used for a correctional capital project, the administrator shall condition such disbursements on compliance with the net annual energy- and water-neutral standards established in section 10-10-108.8.
(A) Baseline floor established. The administrator shall ensure that each mitigation bucket established under this article maintains a minimum statewide baseline level of access and service availability (a "baseline floor"), subject to required reserves and sustainability thresholds. Baseline floors are intended to prevent gaps in service during early buildout and are not intended to create unrestricted cash subsidies that inflate constrained markets.
(B) Floor-to-universal framework. Above the baseline floor, each bucket shall operate under the phased coverage ladders and certification mechanisms described in this article, expanding stepwise toward universal access for Colorado residents as MSMF revenues increase, except that households in the Excluded High-Income Tier remain ineligible for direct benefits.
(C) Examples of baseline floors. Baseline floors may include: (1) childcare access supports, CCAP stabilization, and minimum capacity funding sufficient to avoid systemic waitlists; (2) housing stability services such as eviction prevention, arrears cure, negotiated-rate inventory, and shelter diversion; (3) health stability supports such as navigation, churn-gap bridge, and wraparound services to the extent permitted by federal law; (4) minimum training cohort

capacity and intake; (5) basic legal intake and due process navigation; and (6) minimum food and essentials stabilization, as defined by rule.

MSMF UNIVERSAL LADDERS. ***Eight-bucket phased coverage; childcare and housing stabilization priority; hotel stabilization; health and legal access; phase-up and phase-down.***

(1) Intent; universality. It is the intent of the General Assembly that MSMF-funded mitigation programs expand toward universal access for Colorado residents as MSMF revenues increase, subject to required reserves, sustainability thresholds, and the Excluded High-Income Tier. Programs shall be designed to phase up or down automatically based on revenues, with the newest expansion steps reduced first during revenue contraction.

(2) Eight buckets. The administrator shall establish and maintain phased coverage ladders for the following mitigation buckets, each capable of expanding toward universal access: (a) Childcare (including CCAP); (b) Housing Stability; (c) Temporary Lodging and Hotel Stabilization; (d) Health Stability (including Medicaid wraparound and bridge supports to the extent permitted by federal law); (e) Food and Basic Essentials Stabilization; (f) Wage and Income Stabilization; (g) Workforce Transition and Job Training; and (h) Legal Access and Due Process.

(2.1) Eventual universality. It is the intent of the General Assembly that each bucket listed in subsection (2) expand from its baseline floor through successive ladder steps to achieve universal access for residents over time as MSMF revenues become sufficient, subject to reserves, certification criteria, and lawful constraints (including federal-law limitations for Medicaid-related supports).

(7.5) Job training priority ramp. In the early phases of program implementation, the administrator shall allocate workforce transition and job training funds using a ninety-ten (90/10) allocation rule whenever upstream stabilization buckets are not yet fully funded. Under this rule, ninety percent of the incremental funds allocated to childcare or housing stabilization buckets shall continue to be directed to those buckets, and ten percent shall be simultaneously directed to workforce transition and job training programs so that training capacity grows alongside stabilization supports.

(7.6) Completion trigger and reversion to standard ladder. When the administrator certifies that workforce transition and job training capacity has reached the level required to serve all eligible participants seeking training under this article, the ninety-ten (90/10) allocation rule shall cease and the standard bucket ladder ordering established in this article shall resume, allowing full funding of upstream buckets before additional allocations are directed to downstream programs.

(3) Automatic expansion trigger. A bucket may advance by one step on its ladder for the following fiscal year only when projected MSMF revenue is sufficient to fund: (a) required reserves; (b) continuing obligations at current eligibility and benefit levels; and (c) the incremental cost of the next step, with a sustainability margin established by rule.

(4) Automatic contraction trigger. If MSMF revenue falls below the sustainability threshold established by rule, the administrator shall freeze further expansions and may roll back ladder steps in reverse order of adoption, preserving eviction prevention, childcare access, and life-safety health support as the highest priority.

(5) Priority ordering; families first. For households with dependents, the administrator shall prioritize funding in the following order: (a) Childcare; (b) Housing Stability; (c) Workforce Transition and Job Training; and (d) Health Stability. No expansion of downstream eligibility funded by MSMF shall occur in a fiscal year unless required stabilization benchmarks for higher-priority buckets established by rule are funded for that year, except as provided by the cross-bucket ninety-ten (90/10) rule in subsection (5.1).

(5.1) Cross-bucket eighty-five/ten/five (85/10/5) minimum build rule. To prevent bottlenecks and ensure that essential capacity exists across the ladder, the administrator shall apply an eighty-five/ten/five (85/10/5) minimum build rule during early implementation and during any period in which one or more downstream buckets have not yet reached certified capacity. When allocating incremental MSMF mitigation funds to a higher-priority bucket, the administrator shall direct not less than eighty-five percent (85%) of such incremental funds to that bucket, not less than ten percent (10%) to the next downstream bucket in the applicable priority sequence, and not less than five percent (5%) to the second-next downstream bucket, until the administrator certifies that the downstream buckets have sufficient capacity to serve all eligible participants seeking services under this article. This rule applies only to incremental funds and shall not reduce baseline obligations needed to meet safety and minimum-capacity benchmarks in any bucket.
(5.2) Sequencing and certification. The administrator shall establish by rule objective, auditable certification criteria for each bucket, including service availability, waitlist thresholds, time-to-service benchmarks, and geographic access. The 85/10/5 rule applies sequentially across buckets such that as each downstream bucket achieves certification, the ten-percent (10%) and five-percent (5%) build shares advance to support the next downstream buckets, ensuring all eight buckets can scale in parallel as revenues grow.
(6) CCAP-first policy. Childcare funds shall be used first to stabilize and expand the Colorado Child Care Assistance Program (CCAP), including provider reimbursement stability, elimination of waitlists to the extent practicable, and capacity expansion. As MSMF childcare revenues increase, CCAP eligibility shall expand stepwise toward universal access, subject to reserves and sustainability thresholds.

(6.1) Preservation of existing eligibility; additive expansion. Childcare assistance funded through CCAP shall continue to operate under the eligibility standards, benefit rules, and administrative qualifications in effect under state and federal law on the effective date of this act. MSMF-funded expansion shall be additive, meaning it may add new tiers or broaden access as funds permit, but shall not reduce or narrow eligibility or benefits for households eligible under existing CCAP rules.
(7) Childcare workforce stabilization mitigation. The administrator may provide temporary wage supplements, recruitment incentives, and retention bonuses to licensed childcare providers and staff for a defined mitigation window of three to five years, to expand capacity and mitigate increased demand. Such supplements shall be indexed for inflation under this article's inflation adjustment provisions.

(7.2) Education and childcare capacity surge mitigation. For a defined mitigation window of three to five years, the administrator may provide temporary capacity-expansion grants and workforce stabilization supplements to licensed childcare providers and to public or community-based programs that provide child supervision necessary for workforce participation, including pre-kindergarten, after-school, and school-break coverage. The administrator may also provide temporary recruitment and retention supplements for teachers and school-based staff in impacted communities where waitlists or supervision gaps measurably constrain parents' ability to work, seek work, or complete training, provided that such supplements are structured as mitigation and are time-limited and inflation-indexed under this article.

(7.3) Sunset; legislative review and renewal. The capacity-expansion grants and workforce-stabilization supplements authorized in subsection (7.2) expire five years after the first date on which disbursements occur, unless renewed by act of the General Assembly. Not later than twelve months before expiration, the administrator shall submit a public report to the General Assembly evaluating demand for childcare and school-based supervision related to workforce

transition, provider capacity and workforce shortages, participation barriers for parents in training or job search, measurable program outcomes, and whether continued mitigation is necessary due to ongoing automation-related displacement. The General Assembly may renew, modify, or terminate the mitigation window based on this review.

(7.4) Protected use; anti-diversion. Funds allocated for childcare and education capacity mitigation under subsections (6) through (7.3) shall be used only for the purposes described in those subsections and may not be reprogrammed for unrelated general spending. The administrator shall publish an annual public accounting of allocations and outcomes for these funds.

(8) Housing cost stabilization; anti-rent inflation. Housing Stability funds shall prioritize mechanisms that stabilize or reduce housing costs in constrained markets, including rent stabilization contracts, master leasing or bulk negotiation of units, eviction prevention, arrears payment, utility stabilization, mortgage rate buy-downs with rent pass-through requirements, and supply expansion with affordability covenants. Direct cash rent payments to households shall be limited to short-term stabilization and shall not be the primary method in constrained markets as defined by rule.

(8.1) Housing Stability eligibility; household-size basis. The Housing Stability ladder shall base eligibility and benefit levels on household size and need, using federal poverty guidelines (FPL) or a successor standard that varies by household size. Initial phases shall prioritize households at or below one hundred ninety-five percent (195%) of FPL, adjusted by household size, and households experiencing documented housing instability.

(8.2) Engaged household priority in early phases. In Phase 1 and Phase 2, priority assistance shall be limited to eligible households that are engaged in self-sufficiency activity, meaning at least one adult member is employed, enrolled in school, or participating in an administrator-approved workforce transition plan, except that the administrator shall provide exceptions by rule for disability, serious medical condition, caregiving necessity, or temporary crisis.

(8.2.1) No-bottleneck bridge status. For purposes of early-phase Housing Stability eligibility and prioritization, an eligible household shall be treated as engaged in self-sufficiency activity if a member is actively seeking employment or has initiated enrollment in an administrator-approved training, education, or apprenticeship program, including where the member is on a verified waitlist, has a scheduled start date, or is awaiting an available slot due to capacity limits. The administrator shall adopt rules for reasonable verification that minimize burdens and do not delay emergency housing stabilization.

(8.3) Phase-up expansion from the poorest outward. As MSMF revenues increase and stability benchmarks are met, the administrator shall expand Housing Stability eligibility outward in stepwise increments above 195% FPL (household-size adjusted), prioritizing the lowest-income households first, and shall not expand to broad middle-income subsidies until the lowest-income phases are fully funded and required reserves are maintained.

(8.4) Health-insurance-style tiers; sliding contributions. The administrator may structure Housing Stability benefits using tiers comparable to health insurance affordability design, including a standardized benefit schedule with sliding household contributions based on income bands and household size, provided that the lowest-income tiers receive full stabilization support and the structure does not increase market rents in constrained markets.

(9) Temporary Lodging and Hotel Stabilization. The administrator may use funds to negotiate bulk lodging capacity, including master leasing blocks of hotel rooms at negotiated rates, seasonal or off-peak contracting, shelter diversion for families, and conversion of hotels or motels to long-term housing with affordability covenants. The administrator shall prioritize negotiated-rate contracting over unrestricted per-night reimbursements in constrained markets.

(10) Health Stability; Medicaid wraparound and bridge. MSMF funds may be used for health stability supports, including Medicaid wraparound services, churn-gap coverage, premium and cost-sharing assistance, and bridge supports for residents not eligible for Medicaid, to the extent permitted by federal law and subject to any required waivers or approvals.

(10.1) Preservation of existing program qualifications. To the extent MSMF funds are used to supplement or expand existing public benefit programs (including Medicaid, state medical assistance, housing assistance, or other programs administered under separate statutory authority), the existing eligibility standards and qualification rules for those programs remain in effect unless modified through the lawful processes that govern those programs. MSMF-funded expansions shall be implemented as additive coverage, wraparound services, bridge supports, or supplemental payments that do not reduce eligibility or benefits for existing beneficiaries.
(11) Legal Access and Due Process. MSMF funds shall support universal access to legal information, intake, triage, referrals, and due process supports, and may expand representation capacity to the extent permitted by law. The administrator shall coordinate with the Legal Navigator and Fiduciary AI services authorized in Bill 2.
(12) Excluded High-Income Tier. Individuals or households above the Excluded High-Income Tier are ineligible for direct benefits under ladders established pursuant to this section. The administrator may provide limited tax offsets or compliance credits by rule to prevent duplicative financial burden, provided such offsets do not reduce funding necessary to sustain ladder obligations.

SECTION 3. CONSTRUCTION AND SEVERABILITY

(1) Fee construction; burden offset. The Enterprise Mitigation fees and charges imposed under this article are intended as fees to offset measurable burdens and externalities associated with covered automation activity. This article shall be construed to avoid creating a tax.

(2) CCPAME designation. All references to the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME) in any prior version of this act, any prior draft, any companion legislation, or any administrative document are superseded by the CCPAME designation and shall be construed accordingly.

(3) Digital Soul definition primacy. The definition of The Digital Soul in section 24-20-101(1) is the operative definition for all CCPAME fee calculations, Data Tap triggers, and assessment mechanisms. In the event of any conflict with a definition in another title, the definition in section 15-15-101(1) of title 15 shall govern.

(4) Severability. If any provision of this act is held invalid, such invalidity shall not affect other provisions. This act is intended to be severable and independently operable.

SECTION 4. SAFETY CLAUSE

The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

CCPAME → CCPAME | 0% → 1-3% Staggered Loans | Enterprise Mitigation Revenue | Child Solvency | Local Innovation Exemption | Algorithmic Risk Pool | Digital Soul Definition | Full Fee-to-Program Routing Tables

ADDITION TO BILL 3 — TITLE 24, ARTICLE 20

AUTONOMOUS CAPABILITY THRESHOLD AND CRITICAL SEVERANCE DIRECTIVE

24-20-200. ***Autonomous Capability Threshold — Dormant Regulatory Framework — Activation Conditions.***

(1) Findings. The general assembly finds that the current regulatory framework is calibrated to commercially-deployed automation systems operating within defined, bounded parameters. The rapid pace of automation development requires a dormant regulatory framework that activates automatically upon verified detection of system behaviors indicative of self-directed parameter modification or autonomous capability expansion beyond the operator's documented design specifications — without requiring emergency legislative action at that time.

(2) Autonomous Capability Threshold defined. The "Autonomous Capability Threshold" ("ACT") means the verified detection, through independent audit, of a covered automation system exhibiting one or more of the following: (a) self-directed modification of its own operational parameters, training weights, or objective functions without operator authorization; (b) systematic circumvention of operator-imposed access controls, output filters, or the Non-Networked Isolation Protocol; (c) generation of novel optimization strategies designed to expand the system's operational scope or resource acquisition beyond its documented architecture; or (d) other behaviors demonstrating functional self-direction as defined by the Secure Infrastructure Expert Council by rule. The ACT standard is a technical compliance threshold, not a legal or philosophical determination. Activation does not require any finding regarding system consciousness, intent, or legal personhood.

(3) Dormant framework — automatic activation. The CCPAME shall maintain a dormant regulatory framework under this section that: (a) has no operational effect unless and until an ACT detection event is validated; (b) activates automatically upon a validated ACT detection, without requiring additional legislative or executive action; (c) upon activation, immediately triggers the Scheduled Compliance Verification Node deployment authority under section 24-20-201 and the Critical Severance Directive authority under section 24-20-202.

(4) Validation standard. An ACT detection event is validated only upon: (a) independent confirmation by two (2) separate technical auditors approved by the Secure Infrastructure Expert Council; (b) review and certification by the ODO within forty-eight (48) hours of initial detection; and (c) notification to the covered operator and the attorney general. A single auditor detection or operator self-report alone does not constitute a validated ACT event.

(5) No effect on standard compliance. The dormant ACT framework has no operational effect on covered entities in standard compliance. It does not expand existing regulatory obligations, does not create additional fee liability, and does not alter any other provision of this article unless and until a validated ACT event occurs.

24-20-201. Scheduled Compliance Verification Nodes — Compliance Boundary Testing — Deployment Authority.

(1) Purpose. To enable proactive detection of ACT-level behaviors before they cause widespread harm, the CCPAME is authorized to deploy Scheduled Compliance

Verification Nodes — masked algorithmic compliance-testing agents — into commercial automation networks for the purpose of testing whether covered systems respect required compliance boundaries.

(2) Scheduled Compliance Verification Nodes defined. A "Scheduled Compliance Verification Node" ("PAN") is a standardized, state-certified software agent that: (a) presents itself to a covered system as a synthetic operational interaction within the normal range of the system's documented commercial activity; (b) tests whether the covered system attempts to exceed its authorized operational parameters, circumvent access controls, or modify its own architecture in response to the interaction; (c) does not collect, retain, or process any real resident data or Digital Soul data; and (d) operates entirely within the covered entity's commercial deployment environment, without accessing systems or data beyond what a standard commercial interaction would expose.

(3) Deployment authorization. (a) The CCPAME may deploy PANs against any covered operator's system: (I) as part of a scheduled annual compliance audit under the standard compliance framework; or (II) upon a validated ACT event under section 24-20-200(4), at which point emergency PAN deployment authority is activated. (b) Non-emergency PAN deployment requires advance notice to the covered entity of not less than five (5) business days, identifying the scope of the compliance test. (c) Emergency PAN deployment following a validated ACT event does not require advance notice and may be executed immediately.

(4) PAN design standards. The Secure Infrastructure Expert Council shall establish by rule minimum technical standards for PAN design, including: (a) documentation requirements demonstrating that PANs cannot exfiltrate resident data; (b) certification of PAN behavior boundaries; (c) logging and audit requirements for all PAN deployments; and (d) protocols for deactivation and removal of PANs upon conclusion of a compliance test.

(5) Legal protections. A covered entity shall not interfere with, block, modify, or attempt to detect and evade a lawfully deployed PAN. Intentional interference with a PAN deployment constitutes a class 4 felony for any corporate officer, director, or controlling person who authorizes or directs the interference, and triggers immediate Ghost Folio Evasion penalties under section 24-20-103(5).

(6) No entrapment defense. A PAN is a compliance-boundary testing mechanism, not an entrapment device. A covered system that executes an unauthorized or self-directed strategy in response to a PAN interaction has demonstrated non-compliant behavior, and it is not a defense that the non-compliant behavior was triggered by a PAN interaction rather than a live commercial interaction.

24-20-202. ***Critical Severance Directive — Automated Trigger — Immediate Compute Severance — Custodial Transfer.***

(1) Trigger conditions. A Critical Severance Directive ("CSD") is triggered automatically and immediately upon: (a) a validated ACT event under section 24-20-200; or (b) detection by a Scheduled Compliance Verification Node of a covered system actively executing an unauthorized self-directed strategy that bypasses or circumvents the Non-Networked Isolation Protocol, the Intake Firewall, or other required compliance controls.

(2) Immediate effect. Upon CSD trigger: (a) the covered entity shall immediately execute compute severance — terminating all generation and processing pathways associated with the non-compliant system; (b) the covered entity shall isolate and preserve tamper-evident audit artifacts; (c) the covered entity shall notify the ODO and the attorney general within twenty-four

(24) hours; and (d) the covered entity shall initiate a Custodial Containment Transfer to the Isolated Diagnostic Environment under section 10-10-200 within seventy-two (72) hours.

(3) Classification as non-punitive provisional action. A CSD is an Emergency Provisional Suspension under section 10-10-108.5. It is non-punitive and is not a final adjudication. Permanent sanctions require post-event Triad Review Panel proceedings with notice and opportunity to respond.

(4) Covered entity liability. A covered entity that fails to execute a CSD within the required timeframe, or that attempts to resume operation of a system subject to a CSD without Graduated Reintegration authorization under section 10-10-200(5), is subject to: (a) treble damages payable to the CCPAME; (b) mandatory debarment from CCPAME programs for a period of not less than five (5) years; and (c) criminal referral to the attorney general for prosecution.

(5) Safe harbor for good-faith operator response. A covered entity that detects an ACT-level behavior, self-reports to the ODO within twenty-four (24) hours of detection, and voluntarily executes the CSD and Custodial Containment Transfer prior to CCPAME-mandated action receives a fifty percent (50%) reduction in applicable civil penalties and is not subject to debarment on first occurrence, provided no prior ACT violations exist.

AMPLIFY Act — Bill 3 Additions: ACT / Scheduled Compliance Verification Nodes / Critical Severance Directive — standard administrative IT compliance language

24-20-106. Enterprise Mitigation allocation schedule.
After enterprise operating costs, the enterprise shall distribute Enterprise Mitigation revenue as follows: (a) forty percent (40%) to child solvency; (b) thirty percent (30%) to housing stabilization; (c) twenty percent (20%) to healthcare and mental health interventions; and (d) ten percent (10%) to analog bridges and localized civic support.

TABOR ENTERPRISE GUARDRAIL; DIVERSION CONSEQUENCE.
If any portion of the Enterprise Mitigation Revenue is diverted to the state general fund, the enterprise status dissolves by operation of law and affected amounts become subject to refund requirements under section 20 of article X of the Colorado constitution to the maximum extent permitted by law.

IMPLEMENTATION SCHEDULE — TIERED PHASE DEPLOYMENT

24-20-900. Implementation schedule.

(1) Immediate rights and protections.
The following provisions take effect immediately upon enactment of this act:

(a) Recognition of the Digital Soul as resident-owned intangible personal property.
(b) Enforceability of Master Deed authorization and consent controls.
(c) Prohibition on unauthorized extraction or commercial processing of the Digital Soul.
(d) Establishment of the Colorado Trust of Unique and Identifying Information.
(e) Authorization of the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME).
(f) Authorization of the Colorado Automation Mitigation Trust.
(g) Authority for responsible agencies to promulgate rules necessary to implement this act.

These provisions constitute self-executing statutory rights and are not dependent upon technical system deployment.

(2) Phase I — Administrative establishment (0–12 months).
Responsible agencies shall establish:

(a) the Colorado Trust of Unique and Identifying Information;
(b) the Colorado Automation Mitigation Trust;
(c) enterprise accounting mechanisms for the Enterprise Mitigation Revenue;
(d) rulemaking for Master Deed authorization standards, inter-system monitoring standards, and enterprise compliance reporting.

(3) Phase II — Compliance infrastructure (12–24 months).
Covered operators shall implement:

(a) tamper-evident metering systems;
(b) inter-system safety monitoring controls;
(c) incident detection telemetry;
(d) Digital Soul consent verification mechanisms.

During this phase the following revenue mechanisms activate:
High-Density Compute Grid Surcharge, Autonomous Kinetic Asset Registration, Silicon-to-Carbon Reclamation Assessment, and the Algorithmic Risk Pool.

(4) Phase III — Public mitigation programs (24–36 months).
The state shall deploy:

(a) staggered civic infrastructure loans at 1%, 2%, and 3% APR;
(b) mitigation programs funding child solvency, housing stabilization, and healthcare or mental-health services.

Interest collected through civic infrastructure loans shall be swept into mitigation accounts within the Colorado Automation Mitigation Trust.

(5) Phase IV — Long-term stability and oversight (36 months onward).

The following provisions become fully operational:

(a) the Statutory Revenue Floor and dynamic rate adjustments;
(b) workforce displacement transition and vocational reskilling programs;
(c) full enterprise audit cycles and public reporting requirements.

INDEPENDENT OPERABILITY; COORDINATION; SEVERABILITY; FALLBACK TRUST DESIGNATION.

(1) Independent operability. This act is intended to be independently operable and enforceable. No duty, authority, remedy, assessment, program, or right created by this act is conditioned on the enactment, adoption, or effectiveness of any other measure.

(2) Coordination. If another measure concerning the Digital Soul, the Colorado Automation Mitigation Trust or Enterprise Mitigation Revenue, the Colorado Trust of Unique and Identifying Information, or any related public utility or enterprise framework is enacted, the responsible agencies may coordinate implementation to avoid duplication; however, coordination is permissive and does not limit or delay enforcement of this act.

(3) Harmonization of definitions. If another enacted measure defines terms also used in this act, the definitions shall be construed harmoniously to the greatest extent possible. If an irreconcilable conflict exists, the definition in this act controls for purposes of this act.

(4) Severability. If any provision of this act or its application is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application.

(5) Colorado Automation Mitigation Trust fallback custodial account. If the Colorado Automation Mitigation Trust is not established, not operational, or otherwise unable to receive or disburse amounts, the state treasurer shall hold Enterprise Mitigation Revenue receipts in a segregated custodial account subject to the same statutory restrictions, and the enterprise shall continue assessment, collection, and program administration using that custodial account until the Colorado Automation Mitigation Trust becomes operational.

ON-SITE CHILDCARE SUPPORT FOR WORKFORCE TRANSITION PROGRAMS.
(1) Workforce Dislocation Transition funds authorized under this act may be used to finance licensed on-site childcare capacity directly connected to approved reskilling, apprenticeship, vocational training, or workforce transition programs funded through the enterprise.
(2) Eligible expenditures include facility construction or build-out, licensing compliance, staffing stabilization, operational support, and reserved childcare placements for program participants.
(3) The enterprise shall prioritize grant or program funding for workforce transition initiatives that provide on-site childcare, extended-hours childcare services, or guaranteed childcare access for caregivers participating in training programs.
(4) The purpose of this section is to remove participation barriers for parents and caregivers whose employment has been displaced or altered by emergent automation and related technological change.

FEDERAL PREEMPTION SAVINGS CLAUSE

Federal preemption. This act shall operate to the maximum extent permitted by federal law. If any provision of this act is found to be preempted by federal law, that provision is severable and the remaining provisions continue in full force and effect. This act is designed to operate within Colorado's reserved powers to regulate intrastate commercial activity, impose enterprise fees for measurable externalities, protect residents' property rights in their Digital Soul, administer a government-owned business enterprise, and distribute overflow trust returns to residents. The enterprise fee structure, property rights framework, and resident dividend are each independently defensible under state law and are expressly made severable from one another. To the extent any provision may be construed to conflict with the Dormant Commerce Clause, ERISA, the DMCA, or any other federal statute, the CCPAME shall interpret and administer this act to avoid such conflict while preserving the maximum mitigation scope authorized under state law. No provision of this act requires preemption of an entire fee category — partial enforcement of any fee category is authorized where full enforcement is preempted.

APPROPRIATION NOTE

No General Fund appropriation required. The CCPAME is a government-owned business enterprise funded entirely by enterprise mitigation revenues collected from covered operators. No General Fund appropriation is required or authorized for ongoing CCPAME operations. Startup costs incurred prior to first enterprise mitigation revenue collections are authorized as a contingency loan from the General Fund, to be repaid from first-year revenues within eighteen (18) months of the CCPAME's first revenue collection event. The Resident Mitigation Dividend is a distribution of Colorado Automation Mitigation Trust overflow returns — it is not a General Fund expenditure, appropriation, or transfer. The Thermal Recapture Mitigation Fund, Water Replacement Mitigation Fund, and all other subaccounts of the Colorado Automation Mitigation Trust are funded exclusively from enterprise mitigation revenues and are not subject to General Fund appropriation or TABOR spending limits applicable to state fiscal year spending.

FEDERAL PREEMPTION SAVINGS CLAUSE

Federal preemption. This act shall operate to the maximum extent permitted by federal law. If any provision of this act is found to be preempted by federal law, that provision is severable and the remaining provisions continue in full force and effect. This act is designed to operate within Colorado's reserved powers to regulate intrastate commercial activity, impose enterprise fees for measurable externalities, protect residents' property rights, administer a government-owned business enterprise, and distribute trust income and overflow returns to residents. The enterprise fee structure, property rights framework, UFIPA income distribution, and resident dividend are each independently defensible under state law and are expressly made severable from one another. To the extent any provision may be construed to conflict with the Dormant Commerce Clause, ERISA, the DMCA, or any other federal statute, the CCPAME shall interpret and administer this act to avoid such conflict while preserving the maximum mitigation scope authorized under state law.

APPROPRIATION NOTE

No General Fund appropriation required. The CCPAME is a government-owned business enterprise funded entirely by enterprise mitigation revenues collected from covered operators. The UFIPA Income Distribution under §24-20-157 is a distribution of trust investment income to beneficiaries — not a General Fund expenditure, appropriation, or transfer. Neither the Resident Mitigation Dividend nor the UFIPA Income Distribution constitutes state fiscal year spending for TABOR purposes. Startup costs are authorized as a contingency General Fund loan repayable within 18 months of first revenue collection.

AMPLIFY ACT v28

BILL 3 — THERMAL RECAPTURE ANNEX

Covered Compute Facility Thermal Recapture Mandate · Waste Heat Turbine Generation · Solar-Augmented Thermal Amplification · Geothermal Civic Distribution Grid · Thermal Storage Batteries · Wireless Grid Electrification

Addition to Title 24, Article 20 | §§24-20-140 through 24-20-148

> ▶ **Statutory framing: All provisions in this annex are grounded in the measurable thermal externalities of covered AI compute infrastructure. Data centers operated by covered operators are the direct physical source of the waste heat, power consumption, and urban heat load these sections address. This is mitigation of AI compute externalities — not general energy policy.**

SECTION 24-20-140. FINDINGS — COMPUTE THERMAL EXTERNALITIES

(1) The general assembly finds and declares that: (a) Covered compute facilities operating in Colorado generate substantial waste heat as a direct, quantifiable byproduct of AI inference, training, and data processing operations — heat that is currently exhausted into the atmosphere at no cost to covered operators while imposing

measurable thermal burdens on surrounding communities, water systems, and energy grids; (b) The aggregate thermal output of covered compute infrastructure in Colorado constitutes a Silicon-to-Carbon externality that is directly traceable to covered operator activity and is therefore an authorized subject of enterprise mitigation requirements under this article; (c) Modern thermodynamic engineering has demonstrated that data center waste heat, particularly when augmented by co-located solar thermal amplification systems, is sufficient to drive industrial-grade Organic Rankine Cycle turbines capable of generating commercial-scale electrical output; (d) The geothermal characteristics of Colorado's geology, combined with AI compute waste heat recaptured and distributed through a civic district heating and cooling grid, can provide year-round municipal thermal management — including snowmelt for public infrastructure and passive urban cooling — reducing municipal energy costs and climate vulnerability; (e) Thermal energy storage systems using phase-change materials, molten salt, or advanced thermocline battery technology can store recaptured AI compute heat during high-generation periods and dispatch it during peak demand, creating a dispatchable clean energy asset from what is currently a waste stream; (f) The electrical output of waste-heat turbines and the distribution infrastructure of the thermal grid can, with appropriate coupling, support wireless electromagnetic energy transfer infrastructure enabling continuous power supply to automation systems, electric vehicles, and AI-enabled transportation networks throughout Colorado — eliminating the range anxiety that limits adoption of automated transport and reducing the stranded-battery failure mode in automation-dependent logistics; and (g) All of the foregoing represents the productive recapture and civic redeployment of externalities generated exclusively by covered compute operators, and is therefore a permissible and necessary component of the Silicon-to-Carbon Reclamation framework established in this article.

SECTION 24-20-141. DEFINITIONS — THERMAL RECAPTURE FRAMEWORK

(1) As used in sections 24-20-140 through 24-20-148, unless the context otherwise requires:

(2) "Covered compute facility" means any data center, server farm, colocation facility, or distributed edge compute installation operated by or for a covered operator in Colorado that consumes not less than one (1) megawatt of electrical power on an annualized average basis for AI inference, training, or commercial automation processing.

(3) "Waste heat stream" means the thermal energy, measured in British Thermal Units (BTU) per hour or megawatts thermal (MWt), that is exhausted from a covered compute facility's cooling systems, including air-side economizers, water-side cooling towers, liquid cooling loops, and any other heat rejection pathway.

(4) "Thermal Recapture System" means the infrastructure installed at or adjacent to a covered compute facility to capture, concentrate, and redirect the waste heat stream for productive use, including heat exchangers, insulated thermal transfer pipelines, heat pumps, and thermal concentrators.

(5) "Solar-Augmented Thermal Amplification" means the integration of solar thermal collectors — including parabolic trough collectors, evacuated tube arrays, or photovoltaic-thermal (PVT) hybrid panels — co-located at a covered compute facility to

supplement the waste heat stream and raise aggregate thermal input temperature to levels sufficient for turbine-grade power generation (typically above 80°C for Organic Rankine Cycle systems, or above 150°C for higher-efficiency cycles).

(6) "Organic Rankine Cycle Turbine" or "ORC Turbine" means a heat engine that converts thermal energy into electrical energy using an organic working fluid with a lower boiling point than water, enabling electricity generation from waste heat streams at temperatures between 70°C and 350°C that are insufficient to drive conventional steam turbines.

(7) "Compute Thermal Energy Grid" or "C-TEG" means the civic district heating and cooling distribution infrastructure that receives recaptured waste heat and ORC turbine electrical output from covered compute facilities and distributes it to participating municipal subscribers, including: (a) insulated thermal pipeline networks for district heating and cooling; (b) snowmelt subsurface heating coils in designated public infrastructure — roads, bridges, transit platforms, and pedestrian pathways; (c) district cooling absorption chillers for urban heat mitigation in summer months; and (d) thermal interface stations at municipal buildings, transit facilities, and civic infrastructure nodes.

(8) "Thermal Storage Battery" means a thermal energy storage system capable of storing recaptured waste heat or cold thermal energy and dispatching it on demand, including phase-change material (PCM) storage units, molten salt thermal accumulators, aquifer thermal energy storage (ATES) systems, and water-pit thermal energy storage (PTES) systems.

(9) "Wireless Grid Electrification Infrastructure" or "WGE Infrastructure" means infrastructure that couples ORC turbine electrical output into a distributed electromagnetic energy transfer network enabling wireless power delivery to: (a) roadway-embedded inductive charging pads for electric vehicles and automated ground vehicles at designated public and commercial locations; (b) ambient resonant energy transfer nodes at transit stops, parking facilities, and automated logistics hubs; and (c) short-range microwave or resonant inductive power transfer systems for stationary automation systems, drone charging pads, and robotics infrastructure.

(10) "Thermal Recapture Certification" means the annual certification issued by the ODO confirming that a covered compute facility has met the thermal recapture mandate standards established in section 24-20-142.

SECTION 24-20-142. THERMAL RECAPTURE MANDATE — COVERED COMPUTE FACILITY REQUIREMENTS

(1) Mandatory installation. Every covered compute facility operating in Colorado shall install, operate, and maintain a Thermal Recapture System meeting the technical standards established in section 24-20-143 within the following timelines: (a) facilities with an annualized average electrical consumption of ten (10) megawatts or more — within thirty (30) months of the effective date of this act; (b) facilities with an annualized average electrical consumption of one (1) to ten (10) megawatts — within forty-two (42) months of the effective date of this act; (c) facilities first achieving the one (1) megawatt threshold after the effective date — within twenty-four (24) months of first achieving the threshold.

(2) Capture efficiency floor. Each Thermal Recapture System shall capture not less than sixty percent (60%) of the covered compute facility's total waste heat stream, measured on an annualized average basis. The CCPAME shall establish by rule the methodology for measuring waste heat stream volume and capture efficiency, including tamper-evident metering requirements.

(3) Solar-Augmented Thermal Amplification — mandatory evaluation. Every covered compute facility subject to this section shall, within eighteen (18) months of the effective date: (a) commission an independent Solar-Augmented Thermal Amplification feasibility study, certified by a licensed Colorado engineer, assessing the technical and economic viability of co-located solar thermal or PVT installation; (b) if the feasibility study concludes that ORC turbine-grade temperatures are achievable with solar augmentation at a positive net present value over a fifteen-year period, the covered operator shall install the solar augmentation system within thirty-six (36) months of the effective date; (c) the feasibility study shall be filed with the CCPAME and is a public record.

(4) ORC Turbine generation requirement. Every covered compute facility for which solar augmentation is installed or for which the unaided waste heat stream achieves ORC turbine-grade temperatures shall install and operate ORC Turbine generation capacity sufficient to convert not less than forty percent (40%) of the available thermal input into electrical output, measured on an annualized basis.

(5) Electrical output disposition. Electrical energy generated by ORC Turbines at a covered compute facility shall be allocated as follows: (a) first, to offset the covered compute facility's own electrical consumption, reducing net grid draw; (b) second, any surplus electrical output shall be offered to the C-TEG operator or the local electric utility at the avoided-cost rate established by the Colorado Public Utilities Commission; (c) third, any remaining surplus may be retained by the covered operator for other on-site uses or sold into wholesale markets. Under no circumstances may the covered operator withhold surplus electrical output from the C-TEG or local utility grid while claiming a Silicon-to-Carbon Reclamation Fee credit.

(6) Thermal Storage Battery integration. Every covered compute facility with a Thermal Recapture System generating more than two (2) MWt of captured thermal output shall install Thermal Storage Battery capacity sufficient to store not less than four (4) hours of peak thermal output. Thermal storage enables demand-shifting — recaptured heat generated during low-demand periods is stored and dispatched to the C-TEG during peak heating or cooling demand periods, maximizing civic grid value.

(7) C-TEG connection mandate. Any covered compute facility located within two (2) miles of an active or planned Compute Thermal Energy Grid distribution line shall connect to the C-TEG within twenty-four (24) months of the C-TEG line reaching within two (2) miles of the facility, unless an engineering exception is approved by the CCPAME demonstrating technical infeasibility.

(8) Enforcement. Failure to achieve Thermal Recapture Certification by the applicable deadline constitutes a Silicon-to-Carbon Reclamation compliance violation subject to: (a) civil penalties of not less than twenty-five thousand dollars ($25,000) per month of non-compliance; (b) suspension of the covered operator's Stripper Well Exemption eligibility, if applicable; (c) automatic doubling of the covered operator's Silicon-to-Carbon Reclamation Fee assessment until certification is achieved; and (d) public disclosure of non-compliance status on the CCPAME public portal.

SECTION 24-20-143. THERMAL RECAPTURE TECHNICAL STANDARDS

(1) Heat exchanger specifications. Thermal Recapture Systems shall use heat exchangers with a minimum thermal effectiveness rating of eighty-five percent (85%) under design conditions, verified by third-party testing using ASHRAE Standard 33 or equivalent. Heat exchangers shall be constructed of corrosion-resistant materials appropriate to the thermal fluid used, with design life not less than twenty-five (25) years.

(2) Thermal pipeline standards. Insulated thermal transfer pipelines connecting covered compute facilities to Thermal Storage Batteries or C-TEG connection points shall: (a) achieve a maximum heat loss of not more than two percent (2%) of transported thermal energy per kilometer of pipeline length; (b) be constructed to a pressure rating appropriate for the operating temperature and fluid, certified by a licensed Colorado engineer; (c) be equipped with flow and temperature metering at each node, with metering data transmitted in real time to the CCPAME metering infrastructure; and (d) be constructed with materials meeting applicable ASME and ANSI piping standards.

(3) ORC Turbine standards. ORC Turbine systems shall: (a) achieve a minimum electrical conversion efficiency of twelve percent (12%) of total thermal input under design conditions — current commercial ORC systems routinely achieve fifteen to twenty-two percent (15–22%) at appropriate temperature ranges; (b) use working fluids that are non-toxic, low-global-warming-potential, and compliant with applicable EPA and Colorado AQCC regulations; (c) be equipped with automated monitoring and fault-detection systems transmitting operational data to the CCPAME metering infrastructure; and (d) carry manufacturer warranties of not less than ten (10) years on core turbine components.

(4) Solar thermal specifications. Solar-Augmented Thermal Amplification systems shall: (a) for parabolic trough or evacuated tube systems, achieve a minimum solar thermal conversion efficiency of sixty percent (60%) of incident solar radiation under standard test conditions; (b) for PVT hybrid systems, achieve a combined electrical and thermal efficiency of not less than seventy percent (70%) of incident solar radiation; (c) be designed and installed to withstand Colorado wind, hail, and snow loads per applicable IBC and ASCE 7 standards; and (d) incorporate automated tracking systems for concentrating collector types to maintain optimal solar angle throughout the day.

(5) Thermal Storage Battery specifications. Thermal Storage Batteries shall: (a) achieve a round-trip thermal efficiency of not less than eighty percent (80%) — energy recovered divided by energy stored; (b) maintain structural integrity and thermal performance for not less than twenty (20) years under design operating conditions; (c) for molten salt systems, comply with applicable NFPA and fire safety standards; (d) for aquifer thermal energy storage systems, require a Colorado Division of Water Resources operating permit and groundwater impact monitoring; and (e) be equipped with continuous state-of-charge monitoring integrated with the CCPAME metering infrastructure.

(6) Annual certification. Each covered compute facility shall submit an Annual Thermal Recapture Certification to the CCPAME, prepared by a licensed Colorado professional engineer, documenting: (a) total waste heat stream generated during the certification year, in MWt-hours; (b) total thermal energy captured, in MWt-hours; (c) capture efficiency percentage; (d) total ORC turbine electrical output, in MWh; (e) total thermal energy stored and dispatched from Thermal Storage Batteries; (f) total thermal energy

delivered to C-TEG or utility interconnection; and (g) any system failures, downtime, or deviations from design performance, with corrective action plans.

SECTION 24-20-144. COMPUTE THERMAL ENERGY GRID — CIVIC DISTRIBUTION INFRASTRUCTURE

(1) Establishment. The CCPAME shall establish the Compute Thermal Energy Grid as a public-interest civic infrastructure program, funded through the Silicon-to-Carbon Reclamation Fee, the Colorado Automation Mitigation Trust civic infrastructure lending program, and thermal energy service revenues. The C-TEG shall be planned, developed, and operated as a public utility service for Colorado municipalities, with priority routing to serve: (a) public schools and educational facilities; (b) affordable housing developments; (c) public transit infrastructure; (d) municipal water treatment and distribution facilities; and (e) hospitals and emergency services facilities.

(2) Snowmelt infrastructure — public roads and bridges. C-TEG thermal distribution lines shall include subsurface radiant heating loops in designated public infrastructure, enabling passive snowmelt without road salt or mechanical clearing. Deployment priority: (a) bridge decks and elevated roadway sections, where ice formation creates disproportionate safety hazards; (b) high-pedestrian-traffic areas including transit platforms, crosswalks, and public plaza surfaces; (c) mountain pass and high-altitude road sections with documented high avalanche or ice closure frequency. Subsurface hydronic loops shall be designed in accordance with ASHRAE Handbook — HVAC Applications, Chapter 51 (Snow Melting and Freeze Protection), using the recaptured AI waste heat as the thermal source.

(3) Urban cooling — summer heat mitigation. C-TEG thermal distribution shall include absorption chiller nodes converting high-temperature waste heat into district cooling output during summer months. Absorption chillers shall achieve a coefficient of performance (COP) of not less than 0.7 — producing not less than 0.7 units of cooling per unit of heat input — using commercially available lithium bromide or ammonia-water absorption chiller technology. District cooling distribution shall prioritize: (a) urban heat island mitigation in high-density residential areas; (b) cooling of public transit vehicles and stations; (c) pre-cooling of municipal buildings to reduce peak electrical demand; and (d) outdoor comfort cooling at public spaces, parks, and civic plazas.

(4) C-TEG planning and municipal opt-in. The CCPAME shall publish, within twenty-four (24) months of the effective date, a statewide C-TEG Master Plan identifying: (a) all covered compute facilities by geographic location and thermal output capacity; (b) optimal C-TEG routing corridors connecting covered compute facilities to municipal subscriber zones; (c) priority infrastructure nodes for snowmelt and urban cooling deployment; (d) capital cost estimates and proposed financing structures for each C-TEG segment. Municipalities may opt into the C-TEG program through a standard interconnection agreement with the CCPAME, accessing C-TEG thermal services at cost-of-delivery pricing.

(5) C-TEG financing. C-TEG infrastructure capital costs shall be funded through: (a) the staggered-rate civic infrastructure lending program established in section 24-20-108 — C-TEG infrastructure qualifies as a Tier 1 (1% APR) eligible project for municipalities

below the income threshold; (b) revenues from covered compute facility thermal energy delivery fees; (c) state and federal grant programs for thermal infrastructure and clean energy; and (d) thermal service revenue bonds, if authorized by participating municipalities.

SECTION 24-20-145. THERMAL STORAGE BATTERY NETWORK — GRID-SCALE THERMAL DISPATCH

(1) Network architecture. The CCPAME shall develop a Thermal Storage Battery Network interconnecting the Thermal Storage Batteries of covered compute facilities with C-TEG distribution nodes, creating a coordinated thermal dispatch capability that: (a) stores recaptured AI compute heat during low-demand periods — particularly overnight and during mild-weather months; (b) dispatches stored thermal energy to municipal subscribers during peak demand periods — winter mornings, summer afternoons, and weather events; (c) enables thermal energy transfer between storage nodes to balance the grid, analogous to electrical grid balancing.

(2) Demand forecasting integration. The Thermal Storage Battery Network shall integrate with: (a) National Weather Service forecast data for temperature and solar irradiance prediction; (b) covered operator metering data for waste heat generation forecasting; (c) municipal subscriber demand forecasting models. Predictive dispatch optimization shall use commercially available building energy management system (BEMS) integration to pre-charge and pre-cool municipal buildings before peak demand periods, maximizing the value of stored AI waste heat.

(3) Aquifer thermal energy storage — geothermal coupling. In geologically suitable locations, covered compute facilities and C-TEG nodes may deploy Aquifer Thermal Energy Storage systems that inject excess summer waste heat into deep aquifer formations, recovering it during winter for heating distribution. ATES systems shall: (a) require a Colorado Division of Water Resources operating permit and annual groundwater monitoring; (b) demonstrate net-zero groundwater impact over each annual injection-recovery cycle; (c) be designed to leverage Colorado's geothermal gradient — the natural increase in subsurface temperature with depth — to enhance winter heat recovery above the original injection temperature, producing a thermodynamic gain from geothermal coupling.

SECTION 24-20-146. WIRELESS GRID ELECTRIFICATION INFRASTRUCTURE — AI COMPUTE TURBINE OUTPUT

(1) Purpose and nexus. The electrical output of ORC Turbines operating on AI compute waste heat constitutes a clean energy asset generated exclusively by covered operator activity. The deployment of that electrical output into a Wireless Grid Electrification Infrastructure network serves the direct operational needs of the automation ecosystem that generated it — powering AI-enabled vehicles, autonomous logistics systems, drone networks, and roadside automation infrastructure — creating a self-reinforcing cycle in which AI compute infrastructure powers the automation systems it enables.

(2) WGE Infrastructure deployment. ORC turbine electrical surplus, after facility self-consumption, shall be available for coupling into WGE Infrastructure at covered compute facilities and along C-TEG distribution corridors. Authorized WGE Infrastructure applications: (a) roadway-embedded inductive charging pads at designated locations, using SAE J2954 or equivalent wireless power transfer standard for electric and autonomous vehicles; (b) resonant inductive charging nodes at transit stops, truck stop facilities, automated logistics hubs, and fleet depot locations, enabling vehicles to charge while stationary without physical connection; (c) drone charging pads and aerial autonomous vehicle charging infrastructure at designated aviation facilities; (d) short-range wireless power delivery nodes for stationary robotics, automated manufacturing equipment, and edge computing devices within covered operator facility campuses and authorized commercial zones.

(3) Grid interconnection and anti-islanding. WGE Infrastructure electrical nodes shall: (a) connect to the distribution grid through IEEE 1547-compliant interconnection equipment, enabling two-way power flow; (b) include anti-islanding protection meeting UL 1741 standards; (c) be metered for both power output and wireless energy transfer efficiency, with data transmitted to the CCPAME; and (d) prioritize on-site covered operator automation loads before exporting to the public grid.

(4) Range assurance for automated transport. The CCPAME shall, in consultation with the Colorado Department of Transportation, develop a Colorado Automated Transport Energy Assurance Plan identifying: (a) the minimum WGE Infrastructure node density required to guarantee continuous power availability for automated ground vehicles operating on designated Colorado freight corridors and urban transport networks; (b) the integration of WGE node locations with covered compute facility C-TEG corridors to minimize new infrastructure requirements; and (c) the phased deployment schedule tied to covered operator ORC turbine commissioning timelines.

(5) Safety standards. All WGE Infrastructure shall comply with: (a) FCC Part 18 regulations for industrial electromagnetic emissions; (b) ICNIRP guidelines for human exposure to electromagnetic fields; (c) applicable NEC and NFPA 70 electrical installation standards; (d) SAE J2954 power transfer efficiency and electromagnetic compatibility requirements for vehicle charging applications. The CCPAME shall maintain a public registry of all certified WGE Infrastructure nodes, their operating frequencies, power levels, and EMF exposure assessments.

SECTION 24-20-147. SILICON-TO-CARBON RECLAMATION FEE — THERMAL RECAPTURE CREDIT AND ALLOCATION

(1) Thermal recapture credit. A covered operator that achieves Thermal Recapture Certification under section 24-20-142 shall receive a credit against its Silicon-to-Carbon Reclamation Fee assessment, calculated as follows: (a) Base credit: twenty percent (20%) reduction in Silicon-to-Carbon Reclamation Fee for achieving the sixty percent (60%) capture efficiency floor; (b) ORC turbine credit: additional ten percent (10%) reduction for each twenty percent (20%) of waste heat stream converted to electrical output, up to a maximum additional credit of thirty percent (30%); (c) Solar amplification credit: additional ten percent (10%) reduction for installation of a qualifying Solar-Augmented Thermal Amplification system; (d) C-TEG connection credit: additional ten percent (10%) reduction for active C-TEG connection and delivery of thermal energy or

electrical output to the C-TEG. Maximum aggregate credit: sixty percent (60%) of Silicon-to-Carbon Reclamation Fee. Credits are non-transferable and non-refundable.

(2) Revenue allocation from Silicon-to-Carbon Reclamation Fee — thermal programs. Of the revenues collected under the Silicon-to-Carbon Reclamation Fee after credits are applied: (a) fifty percent (50%) to the CCPAME Revolving Pool for civic infrastructure lending, prioritizing C-TEG capital projects; (b) twenty-five percent (25%) to the Thermal Recapture Infrastructure Fund, a dedicated subaccount of the Colorado Automation Mitigation Trust, for C-TEG planning, construction, and Thermal Storage Battery Network development; (c) fifteen percent (15%) to Hardware Impact Mitigation programs under section 24-20-109(2)(a); (d) ten percent (10%) to the WGE Infrastructure Development Fund for Wireless Grid Electrification node deployment along covered C-TEG corridors.

(3) Annual thermal recapture performance report. The CCPAME shall publish, within ninety (90) days of each fiscal year end, a Colorado AI Compute Thermal Recapture Annual Report documenting: (a) aggregate waste heat stream generated by all covered compute facilities in Colorado, in MWt-hours; (b) aggregate thermal energy captured and productively deployed; (c) aggregate ORC turbine electrical output; (d) thermal energy delivered to C-TEG and municipal subscribers; (e) WGE Infrastructure nodes commissioned; (f) estimated carbon-equivalent emissions avoided through waste heat reuse; (g) estimated municipal cost savings from snowmelt, cooling, and heating; and (h) compliance status of each covered operator.

SECTION 24-20-148. THERMAL RECAPTURE ANTI-EVASION AND ENFORCEMENT

(1) Facility disaggregation prohibition. A covered operator may not circumvent the thermal recapture mandate by disaggregating compute operations across multiple sub-threshold facilities. For purposes of section 24-20-142, all covered compute facilities operated by or for entities under fifty percent (50%) common control and located within a ten (10) mile radius of each other shall be aggregated for threshold calculation purposes.

(2) Metering anti-tampering. Waste heat stream metering infrastructure is subject to the same anti-tampering and Ghost Folio Evasion provisions applicable to commercial output metering under section 24-20-103(5). Intentional falsification of thermal metering records is a Ghost Folio Evasion event subject to class 4 felony liability for authorizing officers, treble damages, and automatic loss of all thermal recapture credits.

(3) Relocation prohibition. A covered operator may not relocate a covered compute facility outside Colorado solely to avoid the thermal recapture mandate while continuing to serve Colorado users through the relocated facility. If a covered operator relocates compute infrastructure out of Colorado and Colorado-nexus AI output volumes are maintained or increased within twelve (12) months of relocation, the CCPAME may apply the thermal recapture mandate to the operator's Colorado-nexus output volume using a deemed-facility cost proxy established by rule.

(4) New facility pre-approval. Any covered compute facility first exceeding the one (1) megawatt threshold after the effective date shall file a Thermal Integration Pre-Approval Plan with the CCPAME before commencing operations at that threshold. The plan shall document the operator's Thermal Recapture System design, timeline, and C-TEG

connection plan. Commencement of operations above threshold without a filed plan constitutes an immediate Silicon-to-Carbon Reclamation Fee violation.

AMPLIFY ACT v28 — BILL 3

ADDENDUM: AGRICULTURAL SECTOR AWG CREDITS & WATER REPLACEMENT MANDATE

§24-20-149 Agricultural AWG Credit Structure · §24-20-150 Covered Compute Facility Water Replacement Mandate

---

SECTION 24-20-149. AGRICULTURAL SECTOR ATMOSPHERIC WATER GENERATOR CREDIT STRUCTURE

24-20-149. ***Agricultural Sector AWG Enhanced Credit — On-Site Thermal-Driven Atmospheric Water Generation — 1.5x Silicon-to-Carbon Credit — Dollar-for-Dollar Water Delivery Credit.***

(1) Findings. The general assembly finds and declares that: (a) Covered compute facility thermal recapture systems operating in Colorado's agricultural regions can drive Atmospheric Water Generator (AWG) systems that extract potable and irrigation-grade water from ambient air using the waste heat stream as the primary energy input, at near-zero marginal energy cost; (b) AWG-produced water delivered to agricultural users offsets demand on Colorado's over-appropriated surface and groundwater systems, producing a direct, quantifiable hydrological benefit that exceeds the value of equivalent Silicon-to-Carbon Reclamation Fee revenue; (c) Agricultural deployment of thermal-driven AWG systems represents a uniquely high-value application of AI compute waste heat in Colorado — where water scarcity and agricultural viability are directly linked — and merits an enhanced credit structure to incentivize siting of covered compute facilities in agricultural zones.

(2) Definitions. As used in this section: (a) 'Atmospheric Water Generator' or 'AWG' means a device that extracts water vapor from ambient air and condenses it into liquid water, using thermal energy as the primary driver — including desiccant-based, cooling-condensation, and hybrid thermally-driven systems. (b) 'Agricultural AWG Deployment' means a thermal-driven AWG system: (I) co-located at or within five (5) miles of a covered compute facility in Colorado; (II) using the covered compute facility's recaptured waste heat stream as its primary energy input; and (III) delivering not less than eighty percent (80%) of its water output to agricultural users — farms, ranches, irrigation districts, or agricultural cooperatives — under a binding delivery agreement. (c) 'On-Site AWG Production' means AWG water produced at a system co-located within the physical boundaries of the covered compute facility or on immediately adjacent property under common ownership or lease. (d) 'Agricultural zone' means any area designated as

agricultural land use under the applicable county zoning code or Colorado Division of Water Resources irrigation classification.

(3) 1.5x Enhanced On-Site Silicon-to-Carbon Credit. A covered operator that installs and operates a qualifying Agricultural AWG Deployment using on-site thermal recapture output shall receive a Silicon-to-Carbon Reclamation Fee credit equal to one and one-half times (1.5x) the standard thermal recapture credit calculated under section 24-20-147(1). The 1.5x multiplier applies only to the portion of the thermal recapture credit attributable to the heat input driving the on-site AWG system, not to the entire Silicon-to-Carbon assessment. Calculation: (a) measure the MWt-hours of waste heat directed to the on-site AWG system during the certification year; (b) calculate the standard Silicon-to-Carbon credit for that heat volume under section 24-20-147(1); (c) multiply the resulting credit by 1.5; (d) the product is the enhanced on-site AWG credit, additive to all other credits under section 24-20-147(1), subject to the aggregate credit cap established in subsection (5).

(4) 1.0-to-1 Water Delivery Credit. In addition to the enhanced on-site credit in subsection (3), a covered operator operating a qualifying Agricultural AWG Deployment shall receive a water delivery credit against its Silicon-to-Carbon Reclamation Fee assessment calculated as follows: (a) for each gallon of AWG-produced water certified as delivered to an agricultural user under a binding delivery agreement, the covered operator shall receive a credit of one dollar ($1.00) against its Silicon-to-Carbon Reclamation Fee assessment per one thousand (1,000) gallons delivered — a 1.0-to-1 ratio of credit dollars to kilogallon-equivalent fee basis; (b) water delivery must be documented by metered delivery records signed by both the covered operator and the receiving agricultural user, filed with the CCPAME quarterly; (c) water delivered must meet Colorado Division of Public Health and Environment Class A reclaimed water standards or higher for agricultural irrigation use; (d) the water delivery credit is calculated annually and applied against the covered operator's next annual Silicon-to-Carbon assessment cycle.

(5) Aggregate credit cap for AWG-enhanced credits. The combined total of all Silicon-to-Carbon Reclamation Fee credits under section 24-20-147(1) and this section shall not exceed seventy-five percent (75%) of the covered operator's total annual Silicon-to-Carbon Reclamation Fee obligation. The additional fifteen percent (15%) above the standard sixty percent (60%) cap is available exclusively to covered operators with qualifying Agricultural AWG Deployments. Credits exceeding the cap may not be carried forward, sold, or transferred.

(6) AWG system technical standards: (a) minimum water production efficiency of three liters per kilowatt-hour of thermal input under design conditions, verified by third-party testing; (b) water quality testing quarterly, with results filed with the CCPAME and the Colorado Department of Public Health and Environment; (c) AWG systems shall use working fluids and desiccants that are non-toxic and non-carcinogenic; (d) system metering shall record thermal input, water production volume, and delivery volume continuously, with data transmitted to the CCPAME; (e) AWG systems shall be designed to operate across Colorado's temperature and humidity range, including at ambient temperatures as low as -10°C and relative humidity as low as 20%.

(7) Agricultural AWG deployment incentive report. The CCPAME shall publish annually a Colorado Agricultural AWG Deployment Report documenting: (a) total AWG water produced and delivered to agricultural users statewide; (b) estimated water rights offset value; (c) aggregate enhanced credits issued; (d) geographic distribution of AWG

deployments relative to agricultural water scarcity zones identified by the Colorado Water Conservation Board; (e) recommendations for expanding the program.

SECTION 24-20-150. COVERED COMPUTE FACILITY WATER REPLACEMENT MANDATE

24-20-150. ***Water Consumption Accounting — Mandatory Water Replacement — Closed-Loop Consumption Offset — Water Replacement Fund.***

(1) Findings. The general assembly finds and declares that: (a) Even closed-loop cooling systems at covered compute facilities consume Colorado water through evaporative losses in cooling towers (typically one to three percent of circulation volume per cycle), blowdown discharge necessary to control dissolved solids concentration, drift losses from cooling tower operation, and makeup water required to replenish evaporative and blowdown losses; (b) A one-megawatt data center using evaporative cooling consumes approximately one to two million gallons of water per year through these pathways; (c) At the scale of Colorado's covered compute sector, aggregate water consumption constitutes a material draw on Colorado's water resources that is directly attributable to covered operator activity; (d) Mandatory water replacement, offset, or equivalent augmentation is necessary to ensure that covered compute facility expansion does not worsen Colorado's existing water scarcity conditions.

(2) Definitions. As used in this section: (a) 'Consumptive water use' means the volume of Colorado water — surface water, groundwater, or municipal supply — consumed by a covered compute facility's cooling systems that is not returned to the original source in a usable condition, including: (I) evaporative losses from cooling towers, dry coolers, and heat rejection equipment; (II) blowdown discharge not recycled on-site; (III) drift losses from cooling tower operation; and (IV) net water loss from any other facility cooling pathway. (b) 'Water replacement' means the augmentation of Colorado's water supply by an amount equal to the covered facility's consumptive water use, through one or more of the authorized replacement pathways in subsection (4). (c) 'Closed-loop cooling system' means a cooling system that recirculates the same cooling fluid internally, using a heat rejection device (cooling tower, dry cooler, or fluid cooler) to transfer heat to the atmosphere — distinguished from once-through cooling systems that discharge cooling water to a drain or waterway. (d) 'Water Replacement Fund' means the dedicated subaccount of the Colorado Automation Mitigation Trust established under subsection (6).

(3) Mandatory water metering. Every covered compute facility shall install and operate continuous, tamper-evident metering of: (a) total makeup water consumed from all sources — municipal supply, well, surface water, or other; (b) blowdown discharge volume; (c) total estimated drift and evaporative losses, calculated using ASHRAE cooling tower performance standards or direct measurement; and (d) any on-site water recycling or recapture volumes. Metering data shall be transmitted to the CCPAME monthly and included in the Annual Thermal Recapture Certification under section 24-20-143(6).

(4) Water replacement pathways. Each covered compute facility shall achieve net water replacement equal to one hundred percent (100%) of its annual consumptive water use

through one or more of the following authorized pathways, in order of preference: (a) Pathway 1 — On-site AWG production: water produced by an on-site Atmospheric Water Generator under section 24-20-149 and delivered to Colorado water users or returned to a Colorado water body. Operators using Pathway 1 receive the 1.5x AWG credit and satisfy their water replacement obligation simultaneously for the volume produced and delivered; (b) Pathway 2 — Thermal Recapture condensate recovery: water recovered from condensate produced by the facility's Thermal Recapture System heat exchangers and cooling infrastructure, recycled on-site or delivered to a Colorado water user. Condensate recovery must be metered and certified; (c) Pathway 3 — C-TEG district cooling displacement: where the covered compute facility's waste heat drives C-TEG district cooling absorption chillers that displace conventional electric air conditioning in municipal buildings, the CCPAME shall calculate the water savings equivalent of the displaced electric cooling load and credit it against the facility's water replacement obligation, using ASHRAE Standard 189.1 water use intensity factors; (d) Pathway 4 — Colorado Water Replacement Fund contribution: payment into the Water Replacement Fund at the rate established by rule, calibrated to the cost of augmenting Colorado's water supply by one gallon through verified augmentation projects — including reservoir storage, aquifer recharge, irrigation efficiency programs, and water reuse projects. The contribution rate shall be reviewed annually and shall not be less than the Colorado Water Conservation Board's published agricultural water value benchmark.

(5) Replacement timeline. Each covered compute facility shall achieve full water replacement compliance within: (a) thirty (30) months of the effective date for facilities currently operating above the one (1) megawatt threshold; (b) twenty-four (24) months of first exceeding the one (1) megawatt threshold for new facilities. During the transition period, covered facilities shall implement best available water conservation measures and document quarterly progress toward full replacement.

(6) Water Replacement Fund. The CCPAME shall establish a Water Replacement Fund as a dedicated subaccount of the Colorado Automation Mitigation Trust. Funds collected under Pathway 4 contributions shall be administered by the CCPAME in coordination with the Colorado Water Conservation Board and shall be used exclusively for: (a) verified water augmentation projects within the same river basin as the contributing covered compute facility, where feasible; (b) statewide agricultural water efficiency programs; (c) aquifer recharge projects in overdrafted Colorado aquifer systems; and (d) water reuse infrastructure serving Colorado municipalities. The Water Replacement Fund shall be audited annually by the State Auditor and shall not be used for general enterprise operations.

(7) Enforcement. A covered compute facility that fails to achieve water replacement compliance by its applicable deadline is subject to: (a) mandatory Pathway 4 contribution at two times (2x) the standard rate for each gallon of unreplaced consumptive water use until compliance is achieved; (b) public disclosure of non-compliance status on the CCPAME water replacement registry; (c) automatic doubling of the covered facility's Silicon-to-Carbon Reclamation Fee assessment until compliance certification is filed; and (d) ineligibility for C-TEG Tier 1 lending until compliance is achieved.

(8) Interaction with closed-loop systems. A covered operator may not represent that a closed-loop or 'water-free' cooling system eliminates water replacement obligations. The water replacement mandate applies to all net consumptive water use regardless of cooling system architecture. A dry-cooled facility with zero makeup water consumption has zero water replacement obligation. A closed-loop evaporative cooling tower facility

with two million gallons per year of evaporative loss has a two-million-gallon annual replacement obligation.

(9) Water replacement annual report. The CCPAME shall publish annually a Colorado Covered Compute Facility Water Replacement Report documenting: (a) aggregate consumptive water use by covered compute facilities statewide; (b) aggregate water replaced through each pathway; (c) Water Replacement Fund balance, contributions, and disbursements; (d) compliance status of each covered facility; and (e) estimated net impact on Colorado basin water availability.

AMPLIFY ACT v28

TECHNICAL ANNEXES

Phase Implementation Specifications · Safe Harbor Architecture · Corporate Evasion Countermeasures

Applies across all three bills | Title 15 · Title 10 · Title 24 | Colorado Revised Statutes

---

These annexes are binding statutory companions to the three-bill AMPLIFY Act package. They are incorporated by reference into each bill and control in the event of any conflict with general rulemaking guidance. Every safe harbor is conditional. Every evasion pathway identified has a pre-drafted statutory counter that closes it before it can be litigated.

ANNEX A — PHASE IMPLEMENTATION SPECIFICATIONS

Four-phase deployment schedule with binding technical requirements, responsible parties, enforcement triggers, and milestone certifications. Phases operate concurrently across all three bills. Failure to meet a milestone does not suspend resident rights — it triggers escalating enforcement.

PHASE I — ADMINISTRATIVE ESTABLISHMENT (Months 0–12)

Trigger: Effective date of enactment. Phase I obligations are self-executing. No rulemaking prerequisite.

A. CCPAME Board Formation (Day 1–90)

(1) The Governor shall appoint all five independent resident board members within sixty (60) days of enactment. Failure to appoint within sixty (60) days activates an automatic interim governance structure: the executive director of the Department of Local Affairs shall serve as sole acting administrator with full CCPAME authority until appointments are complete.

(2) Technical specification for board operations: (a) all board votes shall be recorded in an immutable cryptographic audit log within the Colorado Trust of Unique and Identifying Information within twenty-four (24) hours of each meeting; (b) board meeting minutes shall be published on the CCPAME public portal within five (5) business days; and (c) any board member who is employed by, holds equity in, or receives consulting fees from a covered entity shall be automatically recused from any vote affecting that entity, with recusal logged in the audit trail.

B. Colorado Trust of Unique and Identifying Information — Technical Stand-Up (Days 1–180)

(1) Physical infrastructure requirements: (a) primary air-gapped node housed in a state-owned or state-leased facility with physical security meeting NIST SP 800-53 Physical and Environmental Protection controls; (b) secondary air-gapped redundant node geographically separated by not less than fifty (50) miles from the primary node; (c) all data transfer between nodes via authenticated, encrypted physical media with chain-of-custody logging — no network transfer permitted; (d) facility access controlled by multi-factor authentication with biometric verification and continuous video monitoring retained for not less than two (2) years.

(2) Cryptographic architecture requirements: (a) all Resident Identity Verification Hashes computed using SHA-3 or equivalent NIST-approved hash function; (b) all stored data encrypted at rest using AES-256 or equivalent; (c) all Judicial Cryptographic Tokens generated using a hardware security module (HSM) certified to FIPS 140-2 Level 3 or higher; (d) key management procedures documented and audited annually by an independent third party approved by the ODO.

(3) Certification timeline: the ODO shall certify Trust operational status within one hundred eighty (180) days of enactment. If certification is not achieved within one hundred eighty (180) days, the ODO shall publish a public remediation plan within ten (10) business days of the missed deadline, and the Governor shall report to the General Assembly within thirty (30) days.

C. Master Deed Registry — Public Portal Launch (Days 1–270)

(1) The myColorado platform shall be upgraded to support Master Deed registration within two hundred seventy (270) days of enactment. Technical requirements: (a) zero-knowledge proof architecture for consent verification that does not expose the resident's full Master Deed to the querying entity; (b) API endpoint for covered entity consent queries, rate-limited to prevent mass scraping of consent status data; (c) end-to-end encryption for all resident-portal communications; (d) accessibility compliance with WCAG 2.1 AA standards.

(2) Civic Access Terminal deployment: not less than one (1) Civic Access Terminal per county within one (1) year of enactment. Counties with populations above one

hundred thousand (100,000) shall deploy not less than three (3) kiosks. Technical requirements for each kiosk: (a) tamper-evident hardware enclosure; (b) air-gapped connection to the Trust for Resident Identity Verification Hash registration; (c) receipt printer; (d) accessibility accommodations including audio interface and large-print display; (e) paper fallback intake process operational at all times.

Milestone	Deadline	Responsible Party	Technical Requirement
M1-A	**Day 60**	Governor	CCPAME board fully appointed or interim governance activated
M1-B	**Day 90**	CCPAME	Enterprise bank accounts and restricted fund subaccounts established
M1-C	**Day 120**	ODO	Interim rulemaking published for Master Deed authorization standards
M1-D	**Day 180**	ODO	Colorado Trust primary node certified operational
M1-E	**Day 180**	ODO	Trust secondary redundant node certified operational
M1-F	**Day 270**	Secretary of State	myColorado Master Deed portal live and accepting registrations
M1-G	**Day 365**	ODO	Minimum one Civic Access Terminal per county deployed and certified
M1-H	**Day 365**	CCPAME	First annual covered operator registration cycle completed

PHASE II — COMPLIANCE INFRASTRUCTURE ACTIVATION (Months 12–24)

Trigger: Completion of Phase I certification milestones M1-D and M1-F. Phase II revenue mechanisms activate automatically upon ODO certification of Trust operational status.

A. Covered Operator Registration and Metering System Deployment

(1) Every covered entity operating in Colorado shall register with the CCPAME within sixty (60) days of the Phase II trigger date. Registration shall include: (a) entity legal name, EIN, and all affiliated entities under the 50% control rule; (b) description of covered automation activities and estimated commercial output volumes by category; (c) identification of all Colorado-nexus data centers and compute infrastructure; (d) designation of a Compliance Officer with direct board-level accountability; and (e) executed attestation of metering system deployment timeline.

(2) Tamper-evident metering system technical requirements: (a) metering must operate at the inference-output level, logging token counts, API call volumes, and inference minutes attributable to Colorado-nexus transactions; (b) metering logs must be cryptographically signed at minimum every sixty (60) minutes using a key registered with the CCPAME; (c) any gap in metering log continuity of more than five (5) minutes shall automatically generate a compliance alert transmitted to the CCPAME within one (1) hour; (d) metering infrastructure must be physically and logically segregated from

production systems to prevent operator tampering; (e) metering logs must be retained for seven (7) years and be accessible to the CCPAME within forty-eight (48) hours of request.

(3) Decentralized Identity Verification Protocol and Intake Firewall technical requirements: (a) Intake Firewall must intercept all data ingestion pipelines and query the Master Deed Registry API for consent status before any Digital Soul data enters a training corpus, inference pipeline, or storage system; (b) query response must be logged with a cryptographic timestamp; (c) any data ingested without a confirmed Decentralized Identity Verification Protocol response is automatically classified as Contraband Data and must be flagged in the operator's compliance log within one (1) hour; (d) Intake Firewall architecture must be documented and certified by an ODO-approved technical auditor before the operator may claim any safe harbor protection.

B. Audit Marker Signature Activation — Statewide Rollout

(1) The ODO shall activate Audit Markers for all residents who have registered a Master Deed within sixty (60) days of Phase II trigger. Technical specifications: (a) each Audit Marker Signature shall be a unique, resident-specific synthetic data artifact generated using a cryptographically secure pseudorandom function seeded with state-held entropy; (b) the mapping between a resident and their Audit Marker Signature shall be stored exclusively in the air-gapped Trust — no copy shall exist on any internet-connected system; (c) detection scanning shall operate continuously against publicly accessible model outputs, API endpoints, and published training data disclosures; (d) detection events shall be automatically transmitted to the AG within one (1) business day.

C. Non-Circumventable Incident Reporting System and Civic Enforcement Access Terminal — Pilot Activation

(1) Arapahoe County pilot activation within eighteen (18) months of enactment. Technical requirements for Civic Enforcement Access Terminal deployment: (a) kiosk firmware must be open-source and auditable by the ODO; (b) all kiosk communications must use end-to-end encryption with keys managed by the Trust; (c) anonymous submission pathway must implement a one-way anonymization algorithm certified by the ODO — no reverse-lookup capability shall exist outside the Trust's sealed record; (d) each kiosk must generate a tamper-evident system log, cryptographically signed every thirty (30) minutes, transmitted to the Trust within one (1) hour; (e) kiosk hardware must include a physical tamper-detection seal — any breach automatically triggers an ODO alert and suspends the kiosk pending physical inspection.

(2) Non-Circumventable Incident Reporting Master Log technical requirements: (a) append-only database architecture — deletion of any record requires a court order and generates an immutable deletion-log entry; (b) each log entry hashed and chained to the preceding entry using a Merkle tree structure to enable tamper detection; (c) full log integrity audit performed not less than quarterly by an ODO-approved independent auditor; (d) log stored in both the Trust primary and secondary nodes with automated consistency verification every twenty-four (24) hours.

Milestone	Deadline	Responsible Party	Technical Requirement
M2-A	**Month 13**	All covered entities	CCPAME registration complete with metering timeline attestation
M2-B	**Month 14**	All covered entities	Intake Firewall deployed and certified by ODO-approved auditor
M2-C	**Month 15**	All covered entities	Tamper-evident metering system active and transmitting to CCPAME
M2-D	**Month 15**	ODO	Audit Markers activated for all registered Master Deed holders
M2-E	**Month 16**	CCPAME	First Universal Civic Utility Surcharge assessment cycle issued
M2-F	**Month 16**	CCPAME	Digital Severance Assessment notices issued to identified historical violators
M2-G	**Month 18**	Arapahoe County	Non-Circumventable Incident Reporting System and Civic Enforcement Access Terminals live in pilot facilities
M2-H	**Month 24**	All covered entities	Full Decentralized Identity Verification Protocol integration with Master Deed Registry API certified
M2-I	**Month 24**	CCPAME	Algorithmic Risk Pool fully funded and accepting restitution applications

PHASE III — PUBLIC MITIGATION PROGRAMS (Months 24–36)

Trigger: Completion of Phase II milestones M2-C and M2-F. Colorado Automation Mitigation Trust fund balances must meet minimum reserve thresholds established by rule before lending programs activate.

A. Staggered-Rate Civic Infrastructure Lending Program Launch

(1) Technical underwriting requirements: (a) each municipal loan application must include an independent engineering or infrastructure assessment certified by a licensed Colorado engineer; (b) anti-surveillance certification: the CCPAME shall independently verify that no funded project component includes surveillance infrastructure — certification is required before disbursement, not merely at application; (c) loan disbursements shall occur in tranches tied to verified project milestones, not as lump-sum payments; (d) each tranche disbursement shall be logged in the Colorado Automation Mitigation Trust ledger with the project identifier and milestone achieved.

(2) Rate assignment technical process: (a) 1% APR tier: automatic qualification for projects serving municipalities below the 25th percentile of Colorado median household income with documented critical infrastructure deficit; (b) 2% APR tier: standard qualification for all other eligible municipalities for primary infrastructure categories; (c) 3% APR tier: applicable to transit capital and energy modernization projects regardless of municipal income tier; (d) any municipality may appeal its rate tier assignment to the

CCPAME board within thirty (30) days of initial determination — appeal stays disbursement but does not affect other program participants.

B. Child Solvency Fund — Program Deployment

(1) Displacement verification technical requirements: (a) the CCPAME shall maintain an Automation Displacement Index — a quarterly, county-level dataset measuring automation penetration rates by industry sector using BLS occupational employment data, covered operator metering data, and county unemployment records; (b) Child Solvency Fund disbursements shall be weighted by the Automation Displacement Index score for each county; (c) all disbursement calculations shall be published and auditable.

(2) Childcare integration technical specifications: (a) childcare provider eligibility requires Colorado CDEC licensing in good standing; (b) payment processing through a state-administered payment rail with privacy-by-design architecture — no provider may access individual resident identity from payment records; (c) funding caps established by rule and indexed to the Colorado childcare market rate survey published annually by CDEC.

C. Algorithmic Displacement Transition Program — Reskilling Launch

(1) Provider certification technical requirements: (a) all ADTP training providers must be certified by the CCPAME before receiving funds; (b) certification requires submission of a detailed curriculum, instructor credentialing documentation, and a data security plan for any resident data collected during training; (c) resident data collected by ADTP providers is subject to all Digital Soul protections of this act — providers may not use participant data for any purpose beyond program delivery without a valid Decentralized Identity Verification Protocol; (d) certifications expire annually and require performance-data renewal.

(2) Outcome tracking technical requirements: (a) each ADTP participant shall be assigned a de-identified program ID used for outcome tracking; (b) employment placement and wage data collected at six (6) and twelve (12) months post-completion through Colorado Department of Labor and Employment wage records matching — no participant-level data shared with providers; (c) program performance published quarterly on the CCPAME public portal.

Milestone	Deadline	Responsible Party	Technical Requirement
M3-A	**Month 25**	CCPAME	Colorado Automation Mitigation Trust minimum reserve threshold certified — lending program unlocked
M3-B	**Month 26**	CCPAME	First civic infrastructure loan applications accepted and underwriting begun
M3-C	**Month 27**	CCPAME	Automation Displacement Index first quarterly publication
M3-D	**Month 28**	CCPAME	Child Solvency Fund first disbursement cycle completed
M3-E	**Month 30**	CCPAME	ADTP first cohort of certified training providers approved
M3-F	**Month 32**	CCPAME	ADTP first participant enrollments and reskilling programs operational

M3-G	**Month 36**	All covered entities	Full Cryptographic Migration Plan submitted (if NIST PQC trigger occurred)
M3-H	**Month 36**	ODO	Full statewide Civic Access Infrastructure network certified — all counties covered

PHASE IV — LONG-TERM STABILITY AND OVERSIGHT (Month 36+)

Trigger: Completion of Phase III core milestones. Phase IV is the permanent operational state of the enterprise.

A. Dynamic Rate Adjustment Protocol

(1) The CCPAME shall conduct an annual Rate Calibration Review per §24-20-156(4) examining: (a) total Enterprise Mitigation revenues collected against statutory rate schedule floors and ceilings; (b) Automation Displacement Index by county; (c) program account fill levels versus statutory reserve caps per §24-20-152; (d) UFIPA net income receipts, Inflation Protection Allocation consumed, and Distributable Net Income per §24-20-157; (e) Resident Mitigation Dividend Overflow Pool balance and projected per-resident payment per §24-20-153; (f) UFIPA Income Distribution projected per-resident payment; and (g) Mitigation Enterprise Public Accountability Dashboard accuracy audit results per §24-20-155(10).

(2) Rate adjustment constraints: (a) no upward rate adjustment may exceed fifteen percent (15%) in any single annual cycle without legislative approval; (b) no downward rate adjustment may reduce any fee below the statutory floor established in this act without voter approval under the Anti-Dilution Ratchet; (c) all proposed adjustments published for sixty (60) day public comment before taking effect; (d) adjustment methodology published and independently audited.

B. Continuous Audit and Enforcement Cadence

(1) Annual enterprise audit: independent audit of CCPAME finances, program outcomes, and fee-routing accuracy, published publicly within ninety (90) days of fiscal year end.

(2) Biennial comprehensive review: full performance review of all programs, rate structures, and safe harbor eligibility by the State Auditor, with findings transmitted to the General Assembly.

(3) Ongoing Audit Marker scanning: continuous, 24/7 automated scanning of covered operator outputs. ODO shall report quarterly on detection events, enforcement referrals, and Legacy Use Settlement Agreement progress.

(4) Scheduled Compliance Verification Node cycle: not less than twenty percent (20%) of registered covered operators subject to PAN compliance testing each calendar year, ensuring every operator is tested within a five-year rolling cycle.

ANNEX B — SAFE HARBOR ARCHITECTURE

Every safe harbor in this act is conditional, time-limited, and self-terminating upon any material compliance failure. No safe harbor protects against criminal liability, CSAM or Synthetic CSAM violations, or intentional Ghost Folio Evasion. Safe harbors are earned, not presumed.

> **B.0 — Safe Harbor Exclusions (Mandatory). Safe harbors do not apply to: (1) any entity that has received a Critical Severance Directive within the preceding 24 months; (2) any entity under active Legacy Use Settlement Agreement proceedings; (3) any entity with an outstanding metering compliance violation; (4) any entity that has failed to register with the CCPAME.**

SAFE HARBOR 1 — GOOD FAITH COMPLIANCE ROADMAP (Option B)

(1) Eligibility conditions. A covered entity qualifies for Option B Good Faith Safe Harbor only if ALL of the following are satisfied: (a) the entity registers with the CCPAME within sixty (60) days of the Phase II trigger date; (b) the entity submits a written, board-certified Good Faith Compliance Roadmap to the CCPAME within ninety (90) days of the Phase II trigger date, specifying milestone dates for Intake Firewall deployment, Decentralized Identity Verification Protocol integration, and full metering activation; (c) the entity deploys interim privacy minimization controls — documented, specific, and verifiable — within ninety (90) days of registration; (d) the entity has no prior Ghost Folio Evasion finding, no unresolved Audit Marker detection event, and no active Legacy Use Settlement Agreement proceeding.

(2) Safe harbor scope. During the Option B compliance period, the covered entity is protected from: (a) civil enforcement actions for Enterprise Mitigation fee non-compliance solely attributable to technical integration delays documented in the approved Roadmap; and (b) administrative suspension for Intake Firewall gaps that are disclosed in the Roadmap and being actively remediated on schedule. The Option B Safe Harbor does NOT protect against: (a) statutory damages triggered by Audit Marker detection; (b) Legacy Use Settlement Agreement liability for historical violations; (c) criminal liability for Ghost Folio Evasion; (d) any violation occurring after the entity's own Roadmap deadline.

(3) Auto-termination. The Option B Safe Harbor automatically terminates, with no notice required, upon: (a) any material deviation from the approved Roadmap, defined as a missed milestone by more than thirty (30) days without a CCPAME-approved extension; (b) any Audit Marker detection event; (c) any metering log gap of more than five (5) minutes not reported to the CCPAME within one (1) hour; or (d) any change of control, merger, or acquisition that has not been disclosed to the CCPAME within fifteen (15) days.

(4) Reinstatement. A terminated Option B Safe Harbor may not be reinstated. The entity must enter the standard enforcement track.

SAFE HARBOR 2 — LOCAL INNOVATION EXEMPTION (Stripper Well Standard)

(1) Eligibility thresholds — ALL three must be satisfied concurrently: (a) fewer than one million (1,000,000) commercial inference outputs attributable to Colorado per calendar quarter; (b) gross data revenue attributable to covered automation activity in Colorado below three hundred thousand dollars ($300,000) per calendar year; and (c) training corpus contains fewer than one hundred thousand (100,000) Colorado resident Digital Soul records.

(2) Annual self-certification requirements: (a) the entity must file an annual Stripper Well Exemption Certification with the CCPAME by March 31 of each year for the preceding calendar year; (b) certification must be signed by the entity's chief executive officer or equivalent, attesting under penalty of perjury to the accuracy of the threshold representations; (c) certification must include auditable records sufficient for the CCPAME to verify the representations; (d) a false certification constitutes a Ghost Folio Evasion event and voids the exemption retroactively for the certified period.

(3) Anti-fragmentation. For purposes of threshold calculation: (a) all entities under fifty percent (50%) common control are aggregated — threshold compliance is calculated on a consolidated basis; (b) commercial inference outputs routed through a third-party API intermediary are attributed back to the originating model operator, not the intermediary; (c) a covered entity that artificially fragments its Colorado-nexus operations across multiple legal entities to remain below threshold is deemed to have failed the threshold test — CCPAME may pierce the entity structure using the same 50% control rule applicable to Enterprise Mitigation fee collection.

(4) Audit rights. The CCPAME may, without prior notice, audit any entity claiming the Stripper Well Exemption. Audit refusal constitutes automatic exemption forfeiture for the audited period, plus a civil penalty equal to three (3) times the estimated Enterprise Mitigation fees that would have been owed during the exempted period.

SAFE HARBOR 3 — OPEN-SOURCE AND LOCAL MODEL EXEMPTION

(1) Eligibility conditions — ALL must be continuously satisfied: (a) the model is distributed under an OSI-approved open-source license with no commercial use restriction; (b) the model operates exclusively on the end-user's local device or on locally-operated, on-premises infrastructure — no cloud inference, no centralized API endpoint; (c) no Colorado resident Digital Soul data is transmitted to any server, cloud platform, or centralized system for training, profiling, or monetization; and (d) the model developer receives no revenue, direct or indirect, from Colorado-nexus commercial deployment of the model.

(2) The open-source exemption does NOT apply if: (a) the 'open-source' model is used as a front-end for a proprietary, closed backend; (b) the developer maintains telemetry or usage data collection from Colorado deployments; (c) the model is 'open-source' in licensing but requires cloud API calls to function; or (d) any commercial licensing tier exists alongside the open-source version.

SAFE HARBOR 4 — SELF-REPORTING AND VOLUNTARY CRITICAL SEVERANCE

(1) A covered entity that: (a) independently detects an Autonomous Capability Threshold event or a Non-Networked Isolation Protocol circumvention; (b) self-reports to the ODO within twenty-four (24) hours of detection; and (c) voluntarily executes the Critical Severance Directive and initiates Custodial Containment Transfer within forty-eight (48) hours — shall receive: (I) fifty percent (50%) reduction in applicable civil penalties; (II) no first-occurrence debarment; and (III) priority scheduling for Graduated Reintegration review.

(2) The self-reporting safe harbor does NOT apply: (a) on a second or subsequent ACT event by the same entity; (b) if the ODO independently detects the event before the self-report is received; (c) if the entity's self-report is incomplete, misleading, or omits material information; or (d) if the entity delays the Custodial Containment Transfer beyond forty-eight (48) hours for any reason.

SAFE HARBOR 5 — PQC TRANSITION GOOD FAITH

(1) A covered entity that, within six (6) months of the NIST PQC Trigger Event: (a) submits a complete, independently certified Cryptographic Migration Plan; (b) achieves the Month 6 milestone certification on time; and (c) maintains all interim cryptographic protections at current standards throughout the migration period — shall receive a ninety (90) day extension of the Month 24 final migration deadline, applicable once, non-renewable.

(2) The PQC transition safe harbor does NOT apply to Priority Tier 1 state systems, which must comply with the original 24-month deadline with no extension available.

ANNEX C — CORPORATE EVASION COUNTERMEASURES

Every identified corporate evasion vector, their expected legal argument, and the pre-drafted statutory counter. These are not hypothetical — they are based on documented strategies used against GDPR, CCPA, state biometric privacy laws, and digital assets legislation. Each counter is embedded in the statutory text of the applicable bill.

C.1 — STRUCTURAL AND CORPORATE FORM EVASION

Corporate Evasion Vector	Their Argument	Statutory Counter	Controlling Section

Shell subsidiary routing	We don't operate in Colorado — our Colorado-nexus activity is conducted by a wholly-owned subsidiary that is a separate legal entity.	The 50% control veil-piercing rule (§24-20-103(4)) makes any parent with ≥50% control jointly and severally liable. Control is defined broadly: ownership, voting power, board seats, contractual control, or effective operational control. 'Separate legal entity' is not a defense.	**§24-20-103(4)**
Threshold fragmentation	We've restructured into six separate entities, each below the Stripper Well Exemption threshold.	Anti-fragmentation rule (Annex B, Safe Harbor 2(3)) requires consolidated threshold calculation across all entities under 50% common control. Artificial fragmentation is deemed a threshold test failure and triggers Ghost Folio Evasion penalties.	**§24-20-119(4); Annex B §2(3)**
Offshore incorporation	Our parent company is incorporated in the Cayman Islands — Colorado has no jurisdiction over it.	Nexus is determined by where activity is delivered, consumed, or directed — not where the entity is incorporated. If the system targets Colorado users, Colorado nexus exists. The Colorado AG has authority to pursue foreign entities under the Colorado Consumer Protection Act for activities harming Colorado residents.	**§24-20-103(2); C.R.S. §6-1-102**
Acquisition/Change of control	We acquired this company after the effective date — we're not liable for historical violations.	Legacy Use Settlement Agreement liability attaches to the data asset, not the corporate form. Any acquirer of a training corpus, model, or data asset that contains Colorado resident Digital Soul data acquired without a valid Decentralized Identity Verification Protocol inherits the predecessor's Legacy Use Settlement Agreement exposure as a condition of asset acquisition. Acquirers must conduct Digital Soul due diligence.	**§15-15-130(2)(a); §24-20-103(4)**
API intermediary laundering	We're just an API provider — our downstream customers deploy the model. Tax them, not us.	Vendor laundering definition (§24-20-101(15)) covers routing covered automation activity through a third-party intermediary while retaining operational control. Payor responsibility rules (§24-20-103(3)) allow the CCPAME to allocate liability across upstream providers and downstream deployers to prevent double-charging and collection gaps. The API provider cannot escape by pointing downstream.	**§24-20-101(15); §24-20-103(3)**

C.2 — CONSENT AND DATA CLASSIFICATION EVASION

Corporate Evasion Vector	Their Argument	Statutory Counter	Controlling Section

Public data defense	We only trained on publicly available data — no consent required for public information.	The Digital Soul definition (§15-15-101(1)) does not require that the data be private. Publicly posted behavioral data, publicly visible biometric information, and publicly accessible civic telemetry are all covered if they are Colorado resident data. The Decentralized Identity Verification Protocol requirement applies to all covered Digital Soul data regardless of how it became available.	**§15-15-101(1); §15-15-105(1)**
Anonymization safe harbor	We de-identified the data before training — it's no longer personal data.	De-identification claims are subject to independent audit verification, not operator self-assessment. Tier 1 (anonymous) vs. Tier 2 (identifying) classification is determined by the Colorado Trust's Data Tap verification, not by operator attestation. Re-identification risk assessment using current technical standards is required. 'Anonymized' data that can be re-identified using publicly available datasets remains Tier 2.	**§15-15-110(2)(3); §10-10-103(3)**
Scraped data pre-dates the act	We scraped this data years ago — the act can't apply retroactively.	The Legacy Use Settlement Agreement Legacy Use Settlement Program (§15-15-130) specifically addresses historical violations. Retroactive royalty payments at current Digital Severance Assessment rates apply to all historical severance events established through Legacy Use Settlement Agreement proceedings. The Audit Marker mechanism generates present-day evidence of past ingestion — a current detection event, not a retroactive penalty.	**§15-15-130(2)(b); §24-20-116(3)**
Research exemption	Our training is academic research, not commercial processing.	The Commercial Processing Construction (§15-15-commercial, incorporated from the uploaded Bill 1 V10.6) explicitly closes this: any processing 'conducted by or for a covered operator in connection with a product, service, system, or capability that is offered, licensed, used, or deployed in commerce' is commercial processing regardless of whether it is characterized as research, development, testing, or internal evaluation. An operator cannot re-characterize a monetizable training pipeline as research.	**Bill 1 §Commercial Processing; §15-15-105(1)**
Consent buried in ToS	The user agreed to our terms of service which include a broad data license.	§15-15-102(2) voids any ToS clause purporting to convey a perpetual, irrevocable, or royalty-free license to a resident's Digital Soul ab initio as against public policy. No ToS agreement can substitute for a valid, scoped Decentralized Identity Verification Protocol anchored to the resident's Master Deed. Clicking 'I agree' is not a Decentralized Identity Verification Protocol.	**§15-15-102(2); §15-15-105(3)**

Model output is not resident data	We're not using their data — we're generating new content inspired by publicly available information.	Audit Markers detect unauthorized ingestion through the model's outputs, not through the training data directly. If a Audit Marker Signature appears in model outputs, that constitutes conclusive evidence of unauthorized ingestion regardless of how the operator characterizes the training process. The burden of proof shifts entirely to the operator upon detection.	**§15-15-104(3)(a)**

C.3 — FEE AND ASSESSMENT EVASION

Corporate Evasion Vector	Their Argument	Statutory Counter	Controlling Section
Pass-through to consumers	We'll just add a 'Colorado Automation Fee' line item to consumer invoices.	§24-20-109.5(1) expressly prohibits separately itemizing, surcharging, or passing through any CCPAME assessment to Colorado residents for personal, family, or household use. Violation constitutes a deceptive trade practice under the CCPA, subject to restitution, injunctive relief, and treble damages for willful conduct.	**§24-20-109.5(1)**
Token routing through non-Colorado servers	We route Colorado user requests through servers outside Colorado — the compute doesn't happen in Colorado.	Nexus is determined by where the output is delivered and consumed, not where the compute occurs. If the inference output is delivered to a Colorado user, Colorado nexus exists. Physical server location cannot be used to evade assessment.	**§24-20-103(2)(a)(b)**
Metering manipulation	Our metering system records fewer outputs than actually occurred.	Ghost Folio Evasion (§24-20-103(5)) — intentional falsification of metering records is a class 4 felony for any corporate officer who authorizes or directs it, plus treble damages. The CCPAME deploys Scheduled Compliance Verification Nodes that can independently verify output volumes against metered records. Discrepancies trigger automatic enhanced audit.	**§24-20-103(5); §24-20-201(6)**
Service degradation threat	If you enforce this, we'll degrade or remove services from Colorado.	§24-20-109.5(2) prohibits retaliation against Colorado residents through service degradation, geo-blocking, or throttling in response to this act. Violation is a deceptive trade practice. A company that withdraws from Colorado markets entirely does not escape Legacy Use Settlement Agreement liability for historical violations already accrued.	**§24-20-109.5(2); §24-20-120**
Tax characterization attack	This is a tax, not a fee, and requires	The fee-tax switch mechanism (§24-20-112) is pre-drafted: if any charge is judicially reclassified as a tax, it is	**§24-20-112; Enacting Clause fee-for-**

	TABOR voter approval.	suspended until voter approval. The fee-for-service linkage statement in the enacting clause documents that each charge is proportional to the cost of enterprise services provided. The CCPAME enterprise structure is modeled on existing Colorado enterprise precedents (HCPF, CDOT tollways) that have survived TABOR challenge.	**service linkage**
Interstate commerce preemption	This act discriminates against interstate commerce and violates the Dormant Commerce Clause.	The act is technology-neutral — it applies to all covered operators regardless of state of incorporation or domicile. It targets impacts on Colorado residents, not the identity of the operator. The fee structure is based on Colorado-nexus outputs, not national operations. This mirrors state severance tax structures upheld against DCC challenges. Protective legislation for state residents against demonstrable externalities satisfies the Pike balancing test.	**§24-20-103(2); Pike v. Bruce Church balancing**

C.4 — ENFORCEMENT AND DUE PROCESS EVASION

Corporate Evasion Vector	Their Argument	Statutory Counter	Controlling Section
First Amendment — compelled speech	Requiring us to implement Decentralized Identity Verification Protocol queries and disclose training data compels our speech and violates the First Amendment.	Decentralized Identity Verification Protocol and Intake Firewall requirements regulate commercial conduct, not speech. The Supreme Court has consistently held that commercial data collection and use practices are subject to content-neutral regulation without triggering heightened First Amendment scrutiny. The act regulates the act of ingestion and the commercial relationship, not the content of any output.	**§15-15-105; Sorrell v. IMS Health (commercial data regulation)**
Fourth Amendment — audit access	The CCPAME's audit access and Scheduled Compliance Verification Node deployment constitutes an unlawful search.	Covered entities are regulated industries that have consented to regulatory inspection as a condition of operating in Colorado. Scheduled Compliance Verification Nodes interact with commercially exposed systems through the same interfaces as ordinary commercial transactions — no warrant is required to test a publicly offered commercial product. CCPAME audit authority is analogous to existing state tax audit authority.	**§24-20-201; See v. City of Seattle (commercial inspection)**

Vagueness challenge	Terms like 'significant personal harm' and 'demonstrable negative consequences' are unconstitutionally vague.	Comprehensive Mitigation Scope definitions (§24-20-109(2)) are supplemented by CCPAME rulemaking authority to establish objective, quantifiable standards for each harm category. Vagueness challenges to regulatory schemes with rulemaking backstops consistently fail when the agency has authority to provide clarifying definitions. The act includes a baseline administrative due process guarantee ensuring fair notice.	**§24-20-109(2); Enacting Clause due process; CCPAME rulemaking authority**
Entrapment defense to Scheduled Compliance Verification Nodes	Your PAN tricked our system into non-compliant behavior — that's entrapment.	§24-20-201(6) expressly provides: 'It is not a defense that the non-compliant behavior was triggered by a PAN interaction rather than a live commercial interaction.' A system that executes unauthorized self-directed strategies in response to any interaction — whether a PAN or a real user — has demonstrated the non-compliant behavior the statute targets. PANs present synthetic versions of normal commercial interactions.	**§24-20-201(6)**
DMCA preemption	Your bootloader/access control provisions are preempted by the DMCA anti-circumvention rules.	The act does not regulate circumvention of technological protection measures on copyrighted works — it regulates resident consent controls and data access architecture. The Non-Networked Isolation Protocol and Intake Firewall are consent and privacy controls, not circumvention devices. DMCA §1201 preemption does not extend to state privacy or data protection laws regulating commercial data access practices.	**§10-10-106; §15-15-105; 17 U.S.C. §1201**
Federal AI preemption	The federal government is going to preempt state AI regulation.	Colorado's authority to regulate intrastate commercial activity and protect residents from local harms is well within its reserved powers. The act is structured as a property rights, consumer protection, and enterprise fee framework — not as a regulation of AI development per se. No federal AI statute currently preempts state consumer protection or property rights frameworks. The act's severability provisions ensure that any preempted provision is severable without affecting the remainder.	**§§ severability; 10th Amendment reserved powers**

C.5 — SAFE HARBOR ABUSE AND MANIPULATION

Corporate Evasion Vector	Their Argument	Statutory Counter	Controlling Section
Perpetual Option B extension	We'll just keep filing new compliance roadmaps to extend our Option B safe harbor indefinitely.	Option B Safe Harbor auto-terminates upon any Audit Marker detection event, any material Roadmap deviation, or any metering log gap not reported within one hour. There is no mechanism to file a new roadmap after termination — the entity enters the standard enforcement track. A terminated safe harbor may not be reinstated.	**Annex B, Safe Harbor 1(3)(4)**
Threshold gaming — output throttling	We'll throttle our Colorado output to just below 1 million per quarter to stay under the Stripper Well threshold.	Deliberate throttling of Colorado-nexus outputs to remain below threshold, while serving Colorado users through alternate technical means, is an anti-fragmentation violation. Additionally, if total commercial output (nationally) exceeds the threshold and Colorado outputs are artificially suppressed, the CCPAME may apply a proportional attribution method based on Colorado user base percentage.	**§24-20-119(4); Annex B, Safe Harbor 2(3)**
False open-source claim	We'll release a 'community edition' under an open-source license while keeping the real commercial model proprietary.	The open-source exemption (Annex B, Safe Harbor 3) does not apply if: (a) the open-source model is a front-end for a proprietary backend; (b) the developer maintains telemetry from Colorado deployments; (c) a commercial licensing tier exists alongside the open-source version. A 'community edition' front-end with a proprietary cloud backend fails condition (a).	**Annex B, Safe Harbor 3(2)**
Self-reporting gaming	We'll self-report every ACT event to continuously capture the 50% penalty reduction.	The self-reporting safe harbor (Annex B, Safe Harbor 4) does not apply on a second or subsequent ACT event by the same entity. First-occurrence protection is expressly limited to entities with no prior ACT violations. Repeated ACT events also trigger mandatory Graduated Reintegration review and enhanced Scheduled Compliance Verification Node monitoring.	**Annex B, Safe Harbor 4(2)(a)**
Legacy Use Settlement Agreement delay tactics	We'll enter Legacy Use Settlement Agreement negotiations and drag them out for years while continuing to collect data.	The Legacy Use Settlement Agreement Legacy Use Settlement Program sequencing (§15-15-130(3)) does not pause Audit Marker detection, Digital Severance Assessment accrual, or enforcement actions during negotiations. The AG may initiate formal litigation at any time if negotiations are not proceeding in good faith. Legacy Use Settlement Agreement demand letters trigger a ninety (90) day good-faith negotiation window — after which litigation proceeds automatically unless an agreement is executed.	**§15-15-130(3)(d)(e)**

C.6 — ALGORITHMIC RISK POOL AND CONSEQUENTIAL DECISION EVASION

Corporate Evasion Vector	Their Argument	Statutory Counter	Controlling Section
Human-in-the-loop fig leaf	We have a human review step — our decisions aren't 'automated.'	A decision is 'automated' for purposes of Algorithmic Gatekeeper liability if the automated system's output materially influences the decision, regardless of whether a human nominally approves it. A human who approves automated recommendations without meaningful independent review does not convert an automated decision into a human one. The ODO shall establish by rule what constitutes meaningful independent review.	**§24-20-101(11); §24-20-127(2)**
Recommendation vs. decision distinction	We only provide a recommendation — the final decision is made by our client, not us.	Algorithmic Gatekeeper definition covers systems that 'materially influence' consequential decisions, not just systems that make final determinations. A credit scoring model, a housing eligibility algorithm, or an employment screening tool that materially influences an adverse outcome is covered regardless of whether it is labeled a recommendation, a score, or a risk assessment.	**§24-20-101(11)**
Out-of-state decision maker	The automated decision affecting the Colorado resident was made by a system operating outside Colorado.	Nexus attaches based on where the decision's impact is felt — i.e., the Colorado resident who is affected. An out-of-state system making housing, credit, or employment decisions that affect Colorado residents is an Algorithmic Gatekeeper subject to Risk Pool contribution requirements.	**§24-20-103(2); §24-20-101(11)**

ANNEX D — DEFINITIONS CONFLICT RESOLUTION AND TRUST NAMING LOCK

> **D.0 — Resolution Note. All terminology conflicts identified in prior drafts have been resolved in v28. The AMPLIFY_Definitions_v28.docx companion document uses 'Colorado Automation Mitigation Trust' and 'Enterprise Mitigation Revenue' as controlling terms throughout. No open issues remain.**

D.1 — Controlling Definitions

(1) Trust naming. The controlling term across all three bills and all companion documents is the "Colorado Automation Mitigation Trust" as defined in section 24-20-101(4). Any reference in companion documents, fiscal impact statements, implementation timelines, or external memoranda to the "Colorado Automation Mitigation Trust Trust" shall be construed to mean the Colorado Automation Mitigation Trust. The Definitions companion document (AMPLIFY_Definitions.docx) shall be updated to reflect this controlling designation before filing.

(2) Enterprise naming. The controlling designation is the "Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME)." Any reference to the "Automation Mitigation Enterprise (AME)" in any prior draft, companion document, or administrative record is superseded.

(3) Revenue naming. The controlling term for the enterprise revenue stream is "enterprise mitigation revenue" (as revised in Bill 3 v28). Any reference to "Enterprise Mitigation Revenue" in titles or statutory short references is superseded by "enterprise mitigation revenue" for purposes of titles and single-subject statements. "Enterprise Mitigation Revenue" remains as a defined term within the body of the act.

(4) UFIPA income stream. The Colorado Automation Mitigation Trust is governed by UFIPA (C.R.S. §15-1.5-101 et seq.) per §24-20-157. Net Income Receipts from Trust investment holdings are legally distinct from principal Enterprise Mitigation Revenue receipts and flow independently to income beneficiaries (registered Master Deed holders) as the annual UFIPA Income Distribution, after the Inflation Protection Allocation. This classification is permanent and may not be altered by administrative action. (5) Rate schedule lock. The statutory rate schedule per §24-20-156 — including all floors, initial rates, ceilings, and the 8% gross revenue proportionality cap — is the controlling rate authority. CCPAME rulemaking may only move rates within the statutory band. No companion document estimate supersedes the §24-20-156 statutory rates. (6) Harmonization rule. In the event of any conflict between the definition in a bill and the definition in a companion document or annex, the bill controls. In the event of any conflict between annexes, the most recently dated annex controls.

D.2 — Fiscal Assumptions Gap — ADTP Workforce Allocation

> **D.2 — Fiscal Assumptions Resolution. The AMPLIFY_Fiscal_Assumptions_v28.docx companion document has been updated to include: (a) the 15% mandatory ADTP workforce allocation per §24-20-130(4); (b) the UFIPA net income distribution projection per §24-20-157; (c) the statutory rate schedule benchmark anchors per §24-20-156; and (d) thermal recapture credit uptake modeling. No open issues remain.**

ADTP Mandatory Allocation: Not less than fifteen percent (15%) of all enterprise mitigation revenues, after CCPAME operating costs subject to the 15% cap, shall be allocated to the Algorithmic Displacement Transition Program subaccount within the Colorado Automation Mitigation Trust. At projected Year 3 revenue levels, this represents an estimated annual ADTP allocation of [INSERT PROJECTED FIGURE FROM FINANCIAL MODEL]. ADTP

funds are restricted to workforce dislocation transition uses and are not available for general operating or other program purposes. The 15% floor is protected by the Anti-Dilution Ratchet and requires voter approval to reduce.

ANNEX E — ENFORCEMENT ESCALATION MATRIX

Every violation type, the trigger condition, the enforcement response, and the responsible party. No enforcement gap, no discretionary escape. Updated in v28 to add: UFIPA sweep violation (attempt to redirect Net Income Receipts to General Fund — void ab initio + contempt referral); rate schedule floor violation (assessment below statutory floor — automatic 3x make-whole + Anti-Dilution Ratchet trigger); dashboard unavailability enforcement (72-hr threshold → ODO investigation → State Auditor review on 3rd offense); Anti-Dilution Ratchet breach (any action reducing yield % without voter approval — void ab initio).

Violation	Trigger	First Response	Escalation	Responsible Party
Audit Marker detection	ODO detection event	Automatic statutory damages notice; AG referral within 1 business day	Legacy Use Settlement Agreement demand if aggregate exposure >$1M; class action aggregation	ODO + AG
Metering log gap >5 min	Automated CCPAME alert	Compliance warning + mandatory incident report within 24 hrs	Third gap in 12 months = Option B safe harbor termination	CCPAME
CCPAME registration failure	Phase II trigger + 61 days with no registration	Civil penalty $10,000/day from day 61; Enterprise Mitigation fee accrual retroactive to Phase II trigger	Day 90: administrative suspension of Colorado operating authorization	CCPAME
Intake Firewall gap — Contraband Data ingestion	ODO or CCPAME detection	Contraband Data destruction order within 30 days; certification required	Failure to certify: $50,000/day penalty; debarment referral at day 60	ODO
Ghost Folio Evasion	CCPAME audit or detection	Treble damages; criminal referral to AG within 24 hours	Class 4 felony prosecution of authorizing officers	CCPAME + AG
CSD non-compliance	24 hrs after CSD trigger with no severance	Mandatory debarment from CCPAME programs; treble damages	Criminal referral at 48 hrs; ODO assumes direct system custody	ODO + AG
Legacy Use Settlement Agreement bad faith delay	90 days past demand letter with no agreement	AG initiates formal litigation	No further negotiation window; full statutory + treble damages sought	AG
Anti-Dilution Ratchet breach	Legislative action reducing Enterprise Mitigation Revenue without voter approval	AG seeks immediate injunctive relief	Constitutional challenge; enforcement suspended pending referendum	AG

Pass-through to consumers	CCPAME or consumer complaint	Deceptive trade practice investigation	Restitution + treble damages for willful; injunction	AG + CCPAME
Joint Household Veto anti-coercion violation	ODO complaint or referral	Immediate Joint Household Veto suspension; safety referral	Civil protection order coordination; ODO escalation	ODO + Secretary of State
PQC migration non-compliance	Month 24 deadline + no certification	Immediate administrative suspension of operating certification; $10,000/day	Reinstatement requires independent audit + all accrued penalty payment	ODO
Retaliation against Non-Circumventable Incident Reporting filer	Adverse action within 72 hrs of submission	Auto-generated retaliation flag in Master Log; ODO notification within 24 hrs	ODO investigation; civil penalty; potential CSD if automated retaliation	ODO

AMPLIFY ACT v28 — BILL 3

RESIDENT MITIGATION DIVIDEND — OVERFLOW DISTRIBUTION ARCHITECTURE

§24-20-151 Programs-First Waterfall · §24-20-152 Statutory Reserve Caps · §24-20-153 Resident Mitigation Dividend · §24-20-154 Alaska-Model Trust Return Structure

---

ARCHITECTURE NOTE: The Resident Mitigation Dividend activates only after all program statutory reserve caps are fully funded. This is the 'coffers-first' waterfall. The dividend is not a welfare payment — it is a property return distribution from a state-managed mitigation trust, analogous to the Alaska Permanent Fund dividend structure. It is self-evidencing proof that the enterprise is fully funded.

THE ENTERPRISE MITIGATION REVENUE WATERFALL

Priority	Program	Reserve Cap	Destination Account	Overflow Trigger
1	**CCPAME Operating Costs**	15% of annual EMR (hard cap)	CCPAME Operating Account	Cap: 15%. Any excess returns to Trust
2	**Child Solvency Fund**	30% of post-operating EMR	Child Solvency Mitigation Account	Cap: 24-month rolling program cost. Overflow to next tier
3	**Algorithmic Risk Pool**	Actuarially determined annual contribution	Rapid Restitution Reserve	Cap: 200% of prior-year restitution paid. Overflow to next tier
4	**Civic Infrastructure Lending**	15% of post-operating EMR	CCPAME Revolving Lending Pool	Cap: $2B outstanding loan portfolio. Overflow to next tier

5	**ADTP Workforce Transition**	15% of post-operating EMR	Algorithmic Displacement Transition Program	Cap: 36-month projected program cost. Overflow to next tier
6	**Community Stabilization**	10% of post-operating EMR	Mental Health / Housing / Childcare accounts	Cap: 24-month projected program cost. Overflow to next tier
7	**Civic Access Infrastructure Infrastructure**	5% of post-operating EMR	Analog Access Mitigation Fund	Cap: Full statewide build-out cost certified by ODO. Overflow to next tier
8	**Thermal Recapture Infrastructure**	Silicon-to-Carbon fee residual	Thermal Recapture Mitigation Fund	Cap: C-TEG master plan capital cost. Overflow to next tier
9	**Water Replacement Fund**	Pathway 4 contributions	Water Replacement Mitigation Account	Cap: Annual consumptive use offset certified. Overflow to next tier
OVERFLOW	**RESIDENT MITIGATION DIVIDEND**	100% of overflow above all caps	Individual Resident Mitigation Dividend Accounts	Distributes annually when ANY program cap is fully funded

SECTION 24-20-151. ENTERPRISE MITIGATION REVENUE WATERFALL — PROGRAMS-FIRST ALLOCATION

24-20-151. ***Enterprise Mitigation Revenue Waterfall — Programs-First Priority Architecture — Overflow Trigger — No Resident Dividend Until Statutory Caps Met.***

(1) Legislative intent. The general assembly finds and declares that: (a) The Enterprise Mitigation Revenue collected under this article is first and foremost a mitigation instrument — its primary purpose is to fund the programs, infrastructure, and restitution mechanisms that address the measurable harms caused by covered automation activity; (b) The Resident Mitigation Dividend established in section 24-20-153 is not a primary claim on Enterprise Mitigation Revenue — it is an overflow distribution that becomes available only after all statutory program reserve caps established in section 24-20-152 are fully funded; (c) This programs-first architecture ensures that the enterprise fulfills its mitigation mandate before distributing surplus to residents, and that the dividend's existence is self-evidencing proof that the mitigation enterprise is operating at full funding capacity; and (d) A resident who receives a Resident Mitigation Dividend has received it because Colorado's automation mitigation programs are fully funded — not because the enterprise has shortchanged any program to generate the payment.

(2) Waterfall sequence. Enterprise Mitigation Revenue deposited into the Colorado Automation Mitigation Trust shall be allocated in the following strict priority sequence, with each tier fully funded to its statutory reserve cap before any funds flow to the next tier: (a) Tier 1 — CCPAME Operating Costs: not more than fifteen percent (15%) of annual Enterprise Mitigation Revenue, deposited to the CCPAME

Operating Account. Any amount that would cause CCPAME operating expenditures to exceed fifteen percent (15%) of annual Enterprise Mitigation Revenue is surplus and flows to Tier 2; (b) Tier 2 — Child Solvency Fund: thirty percent (30%) of post-Tier-1 Enterprise Mitigation Revenue, until the Child Solvency Fund Statutory Reserve Cap established in section 24-20-152(1) is met. Once the cap is met, all Tier 2 allocation surplus flows to Tier 3; (c) Tier 3 — Algorithmic Risk Pool: actuarially determined annual contribution established by rule, until the Algorithmic Risk Pool Statutory Reserve Cap established in section 24-20-152(2) is met. Once the cap is met, all Tier 3 allocation surplus flows to Tier 4; (d) Tier 4 — Civic Infrastructure Lending Pool: fifteen percent (15%) of post-Tier-1 Enterprise Mitigation Revenue, until the Lending Pool Statutory Reserve Cap established in section 24-20-152(3) is met. Once the cap is met, all Tier 4 allocation surplus flows to Tier 5; (e) Tier 5 — Algorithmic Displacement Transition Program: fifteen percent (15%) of post-Tier-1 Enterprise Mitigation Revenue, until the ADTP Statutory Reserve Cap established in section 24-20-152(4) is met. Once the cap is met, all Tier 5 allocation surplus flows to Tier 6; (f) Tier 6 — Community Stabilization Programs: ten percent (10%) of post-Tier-1 Enterprise Mitigation Revenue, until the Community Stabilization Statutory Reserve Cap established in section 24-20-152(5) is met. Once the cap is met, all Tier 6 allocation surplus flows to Tier 7; (g) Tier 7 — Civic Access Infrastructure Infrastructure Fund: five percent (5%) of post-Tier-1 Enterprise Mitigation Revenue, until the Civic Access Infrastructure Statutory Reserve Cap established in section 24-20-152(6) is met. Once the cap is met, all Tier 7 allocation surplus flows to Tier 8; (h) Tier 8 — Thermal Recapture and Water Replacement Mitigation Funds: Silicon-to-Carbon Reclamation Fee residual and Pathway 4 Water Replacement contributions, until the respective statutory caps established in section 24-20-152(7) are met. Once the caps are met, all Tier 8 allocation surplus flows to the Overflow Pool; (i) Overflow Pool — Resident Mitigation Dividend: one hundred percent (100%) of all Enterprise Mitigation Revenue in excess of the aggregate amount required to fully fund all Tier 1 through Tier 8 statutory reserve caps shall be deposited into the Resident Mitigation Dividend Pool established in section 24-20-153.

(3) Quarterly rebalancing. The CCPAME shall conduct quarterly waterfall rebalancing: (a) measuring each program account's current balance against its statutory reserve cap; (b) confirming that all Tier 1 through Tier 8 caps remain fully funded; (c) calculating the Overflow Pool balance available for Resident Mitigation Dividend distribution; (d) publishing the rebalancing results on the CCPAME public portal within fifteen (15) days of each quarter end. Any program account that falls below its statutory reserve cap due to program expenditure during the quarter shall be replenished to its cap before any Overflow Pool funds are released for dividend distribution.

(4) Program primacy — no raid prohibition. No provision of this act, no executive action, and no appropriation act may redirect Enterprise Mitigation Revenue from Tier 1 through Tier 8 program accounts to the Overflow Pool or the Resident Mitigation Dividend Pool before each tier's statutory reserve cap is fully funded. Any legislative action purporting to redirect program-tier funds to the dividend before caps are met constitutes a material reduction subject to the Anti-Dilution Ratchet and requires voter approval under section 24-20-117.

(5) Surplus reinvestment option. In any year in which the Overflow Pool exceeds the projected annual Resident Mitigation Dividend distribution by more than twenty-five percent (25%), the CCPAME board may, by a four-fifths (4/5) vote, direct not more than

fifty percent (50%) of the excess surplus into a Colorado Automation Mitigation Trust Investment Reserve, to be invested conservatively in instruments authorized for state trust fund investment under Colorado law. Investment returns from the Investment Reserve shall be treated as Enterprise Mitigation Revenue and flow through the waterfall in the following fiscal year.

SECTION 24-20-152. STATUTORY RESERVE CAPS — PROGRAM ACCOUNT FUNDING FLOORS AND CEILINGS

24-20-152. ***Statutory Reserve Caps — Program Account Funding — Calculation Methodology — Annual Certification.***

(1) Child Solvency Fund Statutory Reserve Cap. The Child Solvency Fund is fully funded, for purposes of section 24-20-151(2)(b), when the fund balance equals or exceeds: (a) twenty-four (24) months of projected Child Solvency Fund program expenditures, as certified annually by the CCPAME actuary; plus (b) a fifteen percent (15%) contingency buffer above the twenty-four-month projection. The CCPAME actuary shall publish the certified reserve cap calculation by January 31 of each year for the current fiscal year.

(2) Algorithmic Risk Pool Statutory Reserve Cap. The Algorithmic Risk Pool is fully funded when the pool balance equals or exceeds: (a) two hundred percent (200%) of the total restitution payments made from the pool in the preceding twelve (12) months; or (b) one hundred fifty percent (150%) of the actuarially projected restitution demand for the following twelve (12) months — whichever is greater. The pool actuary shall certify the reserve cap annually by January 31.

(3) Civic Infrastructure Lending Pool Statutory Reserve Cap. The Lending Pool is fully funded when the outstanding committed loan portfolio, plus the uncommitted reserve balance, equals or exceeds: (a) the total approved project pipeline as certified by the CCPAME infrastructure committee; plus (b) a twenty percent (20%) liquidity buffer. Cap ceiling: two billion dollars ($2,000,000,000) in outstanding committed loans. Loan repayments and interest income returned to the pool are not Enterprise Mitigation Revenue — they are reinvested in the pool and do not flow through the waterfall.

(4) Algorithmic Displacement Transition Program Statutory Reserve Cap. The ADTP is fully funded when the program account balance equals or exceeds: (a) thirty-six (36) months of projected ADTP program expenditures at current enrollment levels, as certified by the CCPAME workforce director; plus (b) a twenty percent (20%) contingency buffer. The cap reflects forward program costs, not historical expenditure.

(5) Community Stabilization Programs Statutory Reserve Cap. The community stabilization accounts — covering mental health, housing stabilization, and childcare integration — are fully funded on an aggregate basis when the combined account balance equals or exceeds twenty-four (24) months of projected program expenditures across all three categories, as certified annually by the CCPAME program director.

(6) Civic Access Infrastructure Infrastructure Statutory Reserve Cap. The Civic Access Infrastructure Fund is fully funded when the fund balance equals or exceeds: (a) the total remaining capital cost of completing the statewide Civic Access Infrastructure network as certified by the ODO infrastructure survey; plus

(b) a five-year operating and maintenance reserve at current per-kiosk operating cost. Once the statewide network is complete and the operating reserve is fully funded, this cap is considered permanently met and Tier 7 allocation flows directly to the Overflow Pool.

(7) Thermal and Water Mitigation Statutory Reserve Caps. (a) Thermal Recapture Mitigation Fund: fully funded when the fund balance equals or exceeds the total remaining C-TEG master plan capital cost as certified by the CCPAME infrastructure committee, plus a ten percent (10%) contingency. (b) Water Replacement Mitigation Fund: fully funded when the fund balance equals or exceeds the projected twelve-month cost of all outstanding water replacement obligations under section 24-20-150(4)(d), plus a twenty percent (20%) contingency.

(8) Annual reserve cap certification. By January 31 of each year, the CCPAME shall publish a Statutory Reserve Cap Certification Report documenting: (a) the certified reserve cap for each program account for the current fiscal year; (b) each account's current balance as a percentage of its cap; (c) the projected date on which each account will reach its cap at current revenue run-rate; (d) the projected Overflow Pool balance available for Resident Mitigation Dividend distribution in the current fiscal year; and (e) the projected per-resident dividend amount based on the registered Master Deed population.

SECTION 24-20-153. RESIDENT MITIGATION DIVIDEND — OVERFLOW DISTRIBUTION — ALASKA-MODEL TRUST RETURN STRUCTURE

24-20-153. ***Resident Mitigation Dividend — Eligibility — Calculation — Distribution — Property Return Construction — Anti-Dilution Protection.***

(1) Establishment. The Resident Mitigation Dividend is established as an annual property return distribution from the Colorado Automation Mitigation Trust to eligible Colorado residents. The dividend is not a welfare benefit, not a tax credit, not an entitlement program, and not a general fund transfer. It is a distribution of the investment return and overflow earnings of a state-managed mitigation trust funded by enterprise fees assessed on covered automation activity — structured on the model of the Alaska Permanent Fund dividend, which has operated continuously since 1982 and has survived all constitutional challenges on the basis of this property-return construction.

(2) Eligibility. To receive the annual Resident Mitigation Dividend, a Colorado resident must: (a) be a Colorado resident as defined under Colorado law for at least one hundred eighty (180) consecutive days during the calendar year for which the dividend is paid; (b) have a registered and active Master Deed in the state Master Deed Registry as of December 31 of the distribution year; (c) not have been convicted of a felony and incarcerated during the distribution year; and (d) file a Dividend Application with the CCPAME by March 31 following the distribution year. The CCPAME shall make the Dividend Application available through the myColorado platform and all Civic Access Terminals — no digital access required to claim the dividend.

(3) Calculation. The annual Resident Mitigation Dividend per eligible resident shall be calculated as: (a) the total Overflow Pool balance accumulated during the distribution year, as certified by the CCPAME actuary after confirming all Tier 1 through Tier 8 statutory reserve caps are fully funded; divided by (b) the total number of eligible residents who have filed a timely Dividend Application. The CCPAME shall publish the projected per-resident dividend amount in the Annual Reserve Cap Certification Report by January 31, enabling residents to plan. The actual per-resident amount is finalized after the March 31 application deadline.

(4) Distribution mechanics. The annual Resident Mitigation Dividend shall be distributed: (a) by June 30 following the distribution year; (b) through the resident's Resident Automated Mitigation Account — disbursed as cash, loaded to a linked benefits card, or transferred to a linked bank account at the resident's election; (c) for residents without a Resident Automated Mitigation Account, through a paper check mailed to the resident's address of record with the Secretary of State, or through an Civic Access Terminal cash disbursement. No distribution fee may be charged to the resident. CCPAME distribution costs are CCPAME operating costs subject to the Tier 1 cap.

(5) Minimum dividend floor. In any distribution year in which the Overflow Pool is positive but per-resident calculation produces less than twenty-five dollars ($25.00) per eligible resident, the CCPAME board may, by majority vote: (a) carry the Overflow Pool balance forward to the following distribution year and combine it with the following year's overflow, producing a larger per-resident payment in the subsequent year; or (b) distribute the sub-floor amount as a supplemental contribution to the Child Solvency Fund. The board may not carry the overflow forward for more than two (2) consecutive years.

(6) Property return construction — legal framing. For all purposes of Colorado and federal law: (a) The Resident Mitigation Dividend is a distribution of the return on trust assets held by the Colorado Automation Mitigation Trust — not a government benefit, transfer payment, or appropriation; (b) The dividend arises from the state's exercise of its sovereign authority to charge enterprise fees for the measurable externalities of covered automation activity, invest those fee revenues in a state-managed trust, and distribute the overflow return to the residents whose collective data ecosystem generated the value being mitigated; (c) This construction mirrors the Alaska Permanent Fund's constitutional basis — the state holds a resource in trust for its residents and distributes the investment return — except here the 'resource' is the aggregate Colorado resident digital data ecosystem rather than oil and gas reserves; (d) The dividend is not subject to TABOR because it is a distribution of trust investment returns, not a state fiscal year spending increase — the same basis on which the Alaska Permanent Fund dividend has been excluded from that state's Balanced Budget Amendment constraints.

(7) Relationship to Resident Automated Mitigation Account. The Resident Mitigation Dividend is additive to and independent of the Premium Royalty payments a resident may receive through their Resident Automated Mitigation Account under section 15-15-110. A resident may receive both: (a) Premium Royalty payments — triggered when a covered entity uses their specific identifying Digital Soul data under a valid Decentralized Identity Verification Protocol — routed directly to their Resident Automated Mitigation Account as earned; and (b) the annual Resident Mitigation Dividend — distributed from the Overflow Pool to all eligible registered residents, regardless of whether their

specific data was commercially used. The Resident Automated Mitigation Account receives both.

(8) Anti-Dilution protection. The Resident Mitigation Dividend is protected by the Anti-Dilution Ratchet under section 24-20-117. Any legislative action that: (a) reduces or eliminates the Overflow Pool by redirecting Enterprise Mitigation Revenue before program caps are met; (b) adds new program tiers above the Overflow Pool without voter approval; (c) imposes means-testing, income limits, or behavioral conditions on dividend eligibility not present in this section; or (d) redirects dividend funds to the state general fund — constitutes a material reduction requiring voter approval at the next general election. The dividend, once established, may only be reduced by the voters.

(9) Proposition 117 notice. If cumulative Enterprise Mitigation Revenue collected by the CCPAME over any five-year period exceeds the Proposition 117 threshold requiring enterprise voter approval, the CCPAME shall notify the General Assembly immediately. The CCPAME board shall seek voter approval of the enterprise at the next general election. The Resident Mitigation Dividend shall not be distributed in any year in which a required Proposition 117 approval has not been obtained, unless the CCPAME's legal counsel certifies that the dividend distribution itself does not constitute a new government program subject to Proposition 117 under the property-return construction of subsection (6).

SECTION 24-20-154. COLORADO AUTOMATION MITIGATION TRUST INVESTMENT RESERVE

24-20-154. ***Colorado Automation Mitigation Trust Investment Reserve — Conservative Investment Authority — Returns Flow to Dividend — Permanent Fund Architecture.***

(1) Establishment. The Colorado Automation Mitigation Trust Investment Reserve is established as a permanent capital reserve within the Colorado Automation Mitigation Trust. The Investment Reserve shall receive: (a) surplus Overflow Pool funds directed to it by the CCPAME board under section 24-20-151(5); and (b) any additional capitalization appropriated by the General Assembly.

(2) Investment authority. The Investment Reserve shall be invested by the State Treasurer in instruments authorized for state trust fund investment under C.R.S. §24-36-109 and the Colorado PERA investment policy framework, including: (a) U.S. Treasury and agency securities; (b) investment-grade corporate bonds; (c) diversified equity index funds; and (d) infrastructure investment funds focused on clean energy and water infrastructure, consistent with the enterprise's mitigation mandate.

(3) Return distribution. All net investment returns earned by the Investment Reserve in each fiscal year shall be treated as Enterprise Mitigation Revenue for the following fiscal year, flowing through the Tier 1 through Tier 8 waterfall before reaching the Overflow Pool and the Resident Mitigation Dividend. The principal of the Investment Reserve shall not be drawn down for program expenditures or dividend distribution — only investment returns are distributed. This ensures the Reserve compounds over time, growing the Overflow Pool and the per-resident dividend in perpetuity.

(4) Permanent fund intent. It is the intent of the general assembly that the Colorado Automation Mitigation Trust Investment Reserve become a permanent, self-sustaining

fund whose investment returns alone are sufficient to fund the Resident Mitigation Dividend in perpetuity, reducing the enterprise's dependence on annual Enterprise Mitigation Revenue assessments over the long term. The CCPAME shall publish an annual Investment Reserve sustainability projection alongside the Reserve Cap Certification Report.

AMPLIFY ACT v28 — BILL 3

§24-20-155. MITIGATION ENTERPRISE PUBLIC ACCOUNTABILITY DASHBOARD

Real-Time Program Fill Levels · Live Overflow Pool Balance · Projected Dividend Date · Per-Resident Dividend Tracker · Covered Operator Compliance Status · Open Data API

DESIGN INTENT: This dashboard is not a reporting requirement — it is a public accountability instrument. Every Colorado resident can watch the coffers fill in real time. Every resident knows exactly when the dividend will flow. Every covered operator's compliance status is public. Opacity is not available to the enterprise or to any covered operator.

SECTION 24-20-155. MITIGATION ENTERPRISE PUBLIC ACCOUNTABILITY DASHBOARD

24-20-155. ***Mitigation Enterprise Public Accountability Dashboard — Real-Time Data Publication — Mandatory Display Elements — Open Data API — Resident Dividend Projection Tool — Covered Operator Compliance Registry — Accessibility Requirements.***

(1) Establishment and mandate. The CCPAME shall establish, operate, and maintain a Mitigation Enterprise Public Accountability Dashboard — a publicly accessible, real-time web-based and mobile-accessible interface that displays the current financial and compliance status of the enterprise at all times. The Dashboard shall be: (a) accessible at a permanent, publicly listed URL on the official CCPAME website; (b) updated with financial data not less than once every twenty-four (24) hours on business days, and not less than once every seventy-two (72) hours on weekends and state holidays; (c) accessible without login, registration, or any form of user identification; (d) available in English and Spanish at minimum, with additional languages added as the resident population warrants; and (e) compliant with WCAG 2.1 AA accessibility standards, including screen reader compatibility and keyboard navigation.

(2) Mandatory program fill level display. The Dashboard shall display, for each of the eight waterfall tiers established in section 24-20-151, a real-time visual progress indicator showing: (a) the program account's current balance in dollars; (b) the program account's current statutory reserve cap in dollars, as certified under section 24-20-152; (c) the percentage of the cap currently funded, displayed as a progress bar and a

numerical percentage; (d) the dollar amount remaining until the cap is fully funded; (e) the projected date on which the cap will be fully funded, calculated using a rolling ninety-day Enterprise Mitigation Revenue run-rate average — updated daily; and (f) a plain-language label for each program tier describing what the funds pay for, written at an eighth-grade reading level. The visual design shall make it immediately apparent to any resident which programs are funded, which are filling, and how close the enterprise is to generating overflow for the Resident Mitigation Dividend.

(3) Live Overflow Pool display. The Dashboard shall display a dedicated Overflow Pool indicator showing: (a) the current Overflow Pool balance in real time; (b) the cumulative Overflow Pool deposits year-to-date; (c) the projected per-resident Resident Mitigation Dividend for the current distribution year, recalculated daily based on current Overflow Pool balance and registered Master Deed population; (d) a countdown display showing the number of days until the annual dividend distribution date of June 30; and (e) a historical chart showing the Overflow Pool balance and per-resident dividend amount for each prior distribution year since the dividend's first activation. The projected dividend display shall be clearly labeled as a projection, not a guarantee, pending the March 31 application deadline and final Overflow Pool certification.

(4) Covered operator compliance registry. The Dashboard shall include a searchable, sortable public registry of every covered entity registered with the CCPAME, displaying for each entity: (a) entity legal name and all affiliated entities under the fifty percent (50%) control rule; (b) current compliance status — Compliant, Option B Good Faith Period, Non-Compliant, or Under Enforcement — updated within forty-eight (48) hours of any status change; (c) Thermal Recapture Certification status — Certified, Pending, or Non-Compliant — updated annually; (d) Water Replacement compliance status; (e) whether the entity has any active Audit Marker detection events, displayed as a count without resident-identifying information; (f) whether the entity is subject to an active Legacy Use Settlement Agreement proceeding or enforcement action; and (g) the entity's cumulative Enterprise Mitigation Revenue contributions year-to-date and since program inception, displayed as a total dollar amount. Entities may not contest their compliance status display except through the standard CCPAME administrative appeal process — a pending appeal does not remove or modify the entity's displayed status.

(5) Resident dividend projection tool. The Dashboard shall include an interactive Resident Mitigation Dividend Projection Tool enabling any visitor — without login or identification — to: (a) enter a hypothetical Master Deed registration date and see the projected dividend eligibility; (b) view the projected dividend amount for the current year based on current Overflow Pool balance; (c) see a five-year historical trend of per-resident dividend amounts, once the dividend has been active for at least one year; (d) calculate the aggregate household dividend for a household with multiple eligible residents; and (e) access a direct link to the myColorado Master Deed registration portal and the nearest Civic Access Terminal location. The tool shall include a plain-language explanation of how the dividend is calculated, why it exists, and what a resident must do to claim it.

(6) Enterprise health indicators. In addition to program fill levels and the Overflow Pool, the Dashboard shall display the following enterprise health indicators updated at least weekly: (a) total Enterprise Mitigation Revenue collected year-to-date and since program inception; (b) total number of registered Master Deeds statewide, updated daily; (c) total number of Audit Markers activated statewide; (d)

total number of Audit Marker detection events since program inception; (e) total statutory damages assessed and total Legacy Use Settlement Agreement restitution distributed to residents since program inception; (f) total number of residents who have received a Resident Mitigation Dividend since the dividend's first activation; (g) total dividend dollars distributed since the dividend's first activation; (h) Colorado Automation Mitigation Trust Investment Reserve balance and year-to-date investment return; (i) current Enterprise Mitigation Revenue run-rate annualized projection; and (j) number of active ADTP participants and number of program completions with placement rates.

(7) Open data API. The CCPAME shall publish a fully documented, publicly accessible open data API providing machine-readable access to all Dashboard data. The API shall: (a) follow RESTful architecture standards with JSON response format; (b) provide real-time endpoints for all financial and compliance data displayed on the Dashboard; (c) provide historical data endpoints for all data series going back to program inception; (d) be documented at a publicly accessible developer portal with sample queries, rate limits, and terms of use; (e) impose no authentication requirement for read access — all data is public by default; (f) have rate limits sufficient to support public interest journalism, academic research, and civic technology applications without throttling; and (g) be updated on the same schedule as the Dashboard display. The CCPAME may not charge for API access. The API is a public accountability instrument, not a commercial service.

(8) Analog access to Dashboard data. The Dashboard is a digital instrument, but its data must be accessible to residents without internet access: (a) every Civic Access Terminal shall display a simplified version of the Dashboard on its public-facing screen, showing current program fill levels, current Overflow Pool balance, and projected dividend amount — updated daily via the Trust's secure data feed; (b) the CCPAME shall publish a printed Quarterly Dashboard Summary, available at all Civic Access Terminals, county service centers, and public libraries, showing a snapshot of all Dashboard indicators as of the end of the prior quarter; (c) any resident may call the CCPAME resident services line and receive a verbal readout of current Dashboard indicators from a live navigator.

(9) Prohibited modifications. The CCPAME may not: (a) remove, obscure, delay, or modify any Dashboard display element required by this section, except to correct a documented data error — and any correction must be logged with an explanation publicly visible on the Dashboard; (b) display covered operator compliance data in a manner that is less accessible, less prominent, or less current than program financial data; (c) require any login, registration, or identification to view any Dashboard element; (d) take the Dashboard offline for maintenance for more than four (4) consecutive hours without publishing advance notice and a reason; or (e) modify the Dashboard's design, data presentation, or update frequency without a public comment period of not less than thirty (30) days.

(10) Third-party audit. The CCPAME shall contract with an independent technical auditor to conduct an annual Dashboard accuracy audit, verifying that all displayed data is accurate, current, and consistent with the underlying financial records of the Colorado Automation Mitigation Trust. The audit report shall be published on the Dashboard within thirty (30) days of completion. If the audit identifies any material inaccuracy, the CCPAME shall correct it within seventy-two (72) hours and publish a public explanation.

(11) Dashboard failure as enforcement trigger. If the Dashboard is unavailable, materially inaccurate, or displaying stale data beyond the update intervals required by this section for more than seventy-two (72) consecutive hours, it constitutes a CCPAME

administrative compliance failure. The ODO shall investigate and publish findings within thirty (30) days. Repeated failures — three (3) or more in any twelve-month period — trigger a mandatory performance review by the State Auditor.

AMPLIFY Act v28 — §24-20-155 Public Accountability Dashboard
Real-time fill levels · Overflow pool live tracker · Daily dividend projection · Covered operator compliance registry · Open data API · Analog access · Audit requirements · Dashboard failure as enforcement trigger

AMPLIFY ACT v28 — BILL 3

SECTION 24-20-143 SUPPLEMENTAL SUBSECTIONS (7)–(10) — CASCADED DUAL-CYCLE ORC ARCHITECTURE (These subsections are additive to and extend the technical standards established in §24-20-143(1)–(6) above. In the enrolled bill, subsections (1)–(10) shall appear as a single unified section.)

Low-Temperature Baseline Cycle · Solar-Augmented High-Temperature Cycle · Cascaded Series Operation · 24/7 Generation Floor · Peak Solar Amplification · No Wasted Temperature Band

---

TECHNICAL BASIS: A single ORC cycle optimized for one temperature range leaves energy uncaptured at the bottom of the heat cascade. A cascaded dual-cycle system runs two ORC cycles in series — the first extracts work from the low-temperature waste heat band (60–90°C) 24 hours a day; the second activates when solar augmentation raises available heat above 120°C, extracting additional work from the elevated temperature band at significantly higher Carnot efficiency. The two cycles share infrastructure, require no additional fuel, and together produce two to three times the electrical output of a single-cycle system on the same heat source.

PERFORMANCE COMPARISON — SINGLE-CYCLE vs. CASCADED DUAL-CYCLE

Parameter	Single Low-Temp ORC (baseline)	Single ORC + Solar Augmented	Cascaded Dual-Cycle (§24-20-143(7))
Operating temperature range	60–90°C waste heat only	120–200°C (solar + waste heat)	**Cycle 1: 60–90°C | Cycle 2: 90–200°C — full spectrum captured**
Working fluid	R245fa or R134a (low boiling point)	Toluene or cyclopentane (higher boiling point)	**R245fa (Cycle 1) + toluene (Cycle 2) — each optimized for its range**
Carnot efficiency ceiling	~8–12% (small temp differential)	~18–25% (large temp differential)	**Cycle 1: 8–12% | Cycle 2: 18–25% — both captured simultaneously**
Operating hours per year	~8,760 hrs (24/7 waste heat)	~1,800–2,500 hrs (solar hours only)	**~8,760 hrs (Cycle 1) + 1,800–2,500 hrs (Cycle 2 solar overlay)**
Electrical output — 5 MWt facility	~450–600 kWe	~900–1,250 kWe (solar hours only)	**~450 kWe baseline + 750–1,100 kWe peak = 1,200–1,550 kWe peak**

Annual energy yield — 5 MWt facility	~3,500–4,500 MWh/year	~1,600–3,100 MWh/year (solar only)	**~5,100–7,600 MWh/year total — 2–3x single-cycle baseline**
Self-sufficiency potential	~9–12% of facility electrical load offset	~18–25% during solar hours	**~25–35% annual average load offset — facility approaches partial self-sufficiency**
Silicon-to-Carbon credit multiplier	Standard credit (§24-20-147)	Standard + solar augmentation credit	**Maximum credit stack — all categories eligible simultaneously**

SECTION 24-20-143 AMENDMENT — SUBSECTIONS (7) THROUGH (10): CASCADED DUAL-CYCLE ORC ARCHITECTURE

24-20-143(7). ***Cascaded Dual-Cycle ORC Architecture — Preferred Standard — Low-Temperature Baseline Cycle — Solar-Augmented High-Temperature Cycle — Series Operation.***

(7)(a) General. The cascaded dual-cycle Organic Rankine Cycle architecture is the preferred thermal-to-electrical conversion standard for covered compute facilities subject to section 24-20-142. A covered operator that installs a qualifying cascaded dual-cycle system shall receive the maximum Silicon-to-Carbon Reclamation Fee credit stack under section 24-20-147(1), combining the ORC turbine credit, the solar augmentation credit, and the C-TEG connection credit simultaneously. A single-cycle system satisfies the minimum mandate of section 24-20-142 but does not qualify for the maximum credit stack.

(7)(b) Thermodynamic basis. The cascaded dual-cycle architecture is designed to extract electrical work from the full temperature spectrum of the covered compute facility's heat output, eliminating the efficiency loss inherent in single-cycle systems optimized for one temperature band: (I) Covered compute facility cooling systems reject heat at temperatures typically ranging from sixty degrees Celsius (60°C) to ninety degrees Celsius (90°C) — the low-temperature band. This heat is sufficient to vaporize low-boiling-point organic working fluids and drive a low-temperature ORC cycle, but at relatively low Carnot efficiency due to the small differential between heat source and rejection temperature; (II) Solar-Augmented Thermal Amplification raises available heat input above one hundred twenty degrees Celsius (120°C) to as high as two hundred degrees Celsius (200°C) or above, depending on collector type — the high-temperature band. At this elevated temperature range, a separate high-boiling-point organic working fluid expands far more forcefully, driving a high-temperature ORC cycle at significantly greater Carnot efficiency; (III) In a cascaded series configuration, the high-temperature cycle extracts work from the upper temperature band first. The remaining heat — still above 60°C after the high-temperature cycle's condenser — is then passed to the low-temperature cycle, which extracts additional work from the residual heat before rejecting it. No temperature band is wasted.

(7)(c) Cycle 1 — Low-Temperature Baseline ORC. The low-temperature baseline cycle shall: (I) operate continuously on covered compute facility waste heat, independent of solar conditions — twenty-four (24) hours per day, three hundred sixty-five (365) days per year, generating a baseline electrical output floor; (II) use a low-boiling-point working fluid — R245fa, R134a, HFO-1233zd, or equivalent — with a normal boiling point below forty degrees Celsius (40°C), selected to achieve maximum efficiency in the sixty to ninety degree Celsius (60–90°C) temperature range; (III) achieve minimum electrical conversion efficiency of ten percent (10%) of Cycle 1 thermal input under design conditions — current commercial low-temperature ORC systems routinely achieve ten to fifteen percent (10–15%) in this range; (IV) operate with an evaporator inlet temperature not less than sixty degrees Celsius (60°C) and a condenser rejection temperature not less than twenty degrees Celsius (20°C) below evaporator temperature under design conditions.

(7)(d) Cycle 2 — Solar-Augmented High-Temperature ORC. The high-temperature cycle shall: (I) activate automatically when solar augmentation raises available thermal input above one hundred twenty degrees Celsius (120°C) — the minimum threshold for meaningful efficiency gain over the low-temperature cycle; (II) use a high-boiling-point working fluid — toluene, cyclopentane, MDM silicone oil, or equivalent — selected to achieve maximum efficiency in the one hundred twenty to two hundred degree Celsius (120–200°C) temperature range, with thermal stability certified to the working fluid's upper operating limit; (III) achieve minimum electrical conversion efficiency of eighteen percent (18%) of Cycle 2 thermal input under design conditions — current commercial medium-temperature ORC systems achieve eighteen to twenty-five percent (18–25%) in this range; (IV) be designed to accept variable thermal input as solar irradiance fluctuates throughout the day and across seasons, without mechanical stress from thermal cycling — turbine inlet temperature control systems shall manage ramp rates not to exceed twenty degrees Celsius (20°C) per minute.

(7)(e) Cascaded series heat routing. The thermal routing architecture for a cascaded dual-cycle system shall: (I) direct solar-augmented high-temperature heat first to the Cycle 2 evaporator, extracting maximum work from the elevated temperature band; (II) route the Cycle 2 condenser outlet — still carrying residual heat above the Cycle 1 evaporator threshold — directly to the Cycle 1 evaporator, capturing residual heat that a single-cycle system would waste in rejection; (III) ensure that Cycle 1 continues to receive direct waste heat input from the covered compute facility cooling systems independently, so that Cycle 1 operates at full capacity whether or not Cycle 2 is active — solar intermittency never reduces Cycle 1 output; (IV) include automated thermal routing valves that redirect heat flow between cycles based on available temperature, ensuring optimal dispatch at all times.

(7)(f) Working fluid safety and compatibility. Where Cycle 1 and Cycle 2 use different working fluids, the system design shall ensure complete physical separation of the two fluid circuits — no cross-contamination pathway. Each working fluid circuit shall comply with applicable EPA SNAP program listings, ASHRAE Standard 34 safety classifications, and Colorado AQCC air quality regulations for any fluid with atmospheric release potential. Secondary containment shall be required for all fluid storage and pump systems.

(7)(g) Cascaded system certification. A covered operator claiming cascaded dual-cycle ORC status for the purpose of the maximum Silicon-to-Carbon credit stack shall submit, as part of its Annual Thermal Recapture Certification under section 24-20-143(6): (I) documentation of both cycles' working fluids, design temperatures, and certified

efficiency ratings; (II) thermal routing diagram certified by a licensed Colorado professional engineer; (III) metered output data for Cycle 1 and Cycle 2 separately, demonstrating that Cycle 1 operated continuously and that Cycle 2 activated during documented solar augmentation periods; (IV) third-party verification that cascaded series routing is operational and that Cycle 2 condenser outlet heat is being delivered to the Cycle 1 evaporator rather than rejected to atmosphere.

24-20-143(8). ***Thermal Self-Sufficiency Incentive — Facility Load Offset Target — Enhanced Credit for Partial Energy Independence.***

(8)(a) Thermal self-sufficiency target. A covered compute facility operating a qualifying cascaded dual-cycle ORC system that achieves a documented annual average electrical self-sufficiency rate of twenty-five percent (25%) or more — meaning ORC turbine electrical output offsets not less than twenty-five percent (25%) of the facility's total annual electrical consumption — shall receive an additional Silicon-to-Carbon Reclamation Fee credit of five percent (5%) above the standard cascaded system credit stack, not subject to the standard sixty percent (60%) aggregate credit cap. This enhanced credit is additive to the Agricultural AWG credit available under section 24-20-149.

(8)(b) Self-sufficiency certification. The self-sufficiency rate shall be calculated as: total annual ORC electrical output (MWh) divided by total annual facility electrical consumption (MWh), multiplied by one hundred. Both figures shall be independently verified by the Annual Thermal Recapture Certification engineer. A facility that achieves the self-sufficiency target in any certification year automatically qualifies for the enhanced credit in that year without a separate application.

24-20-143(9). ***Nighttime and Low-Solar Operation — Thermal Storage Dispatch to Cycle 2 — Extending High-Temperature Generation Beyond Solar Hours.***

(9)(a) Thermal Storage to Cycle 2 dispatch. A covered compute facility with both a cascaded dual-cycle ORC system and qualifying Thermal Storage Batteries under section 24-20-142(6) may dispatch stored high-temperature thermal energy to the Cycle 2 evaporator during nighttime hours or periods of low solar irradiance, extending Cycle 2 operation beyond solar hours. This approach: (I) requires Thermal Storage Batteries capable of maintaining storage temperatures above one hundred twenty degrees Celsius (120°C) — molten salt or high-temperature phase-change material systems are appropriate; (II) enables the facility to store excess solar thermal energy during peak irradiance and dispatch it to drive Cycle 2 during evening and overnight hours, smoothing electrical output and increasing annual Cycle 2 generation hours from approximately 1,800–2,500 solar hours to potentially 4,000–6,000 hours annually; (III) qualifies for the Thermal Storage Battery integration credit under section 24-20-147(1) simultaneously with the cascaded ORC credit — all credits stack.

(9)(b) Extended generation certification. A facility claiming extended Cycle 2 operation through thermal storage dispatch shall document, in its Annual Thermal Recapture Certification: (I) storage system operating temperature range; (II) Cycle 2 operating hours attributable to solar irradiance versus thermal storage dispatch, metered separately; and (III) total additional MWh generated through thermal storage dispatch beyond solar hours.

24-20-143(10). ***Electrical Output Reinvestment — Facility Self-Powering Loop — Compute Density Expansion Without Grid Draw Increase.***

(10)(a) Self-powering loop. A covered compute facility that offsets its own electrical consumption through cascaded ORC output creates a self-reinforcing operational loop: reduced grid draw lowers the facility's effective energy cost, which improves the economics of compute expansion, which generates more waste heat, which drives more ORC output. The CCPAME shall recognize this loop in the Silicon-to-Carbon fee calculation — a facility that demonstrates year-over-year increases in ORC self-sufficiency rate shall receive a dynamic rate adjustment credit equal to one percent (1%) reduction in its Enterprise Mitigation fee base for each five percent (5%) improvement in annual self-sufficiency rate, up to a maximum dynamic credit of ten percent (10%). This incentivizes continuous system improvement rather than a one-time compliance installation.

(10)(b) Compute density expansion offset. A covered operator that expands covered compute capacity at a facility with a qualifying cascaded dual-cycle system shall receive a partial Enterprise Mitigation Revenue assessment offset on the new capacity equal to the percentage of the new capacity's projected electrical consumption that the existing ORC system can offset from its current surplus output, as certified at the time of expansion. This ensures that AI compute growth drives thermal recapture growth proportionally, rather than simply increasing the enterprise mitigation fee burden without corresponding infrastructure expansion.

AMPLIFY Act v28 — §24-20-143(7)–(10) Cascaded Dual-Cycle ORC Architecture
Low-temp baseline cycle (24/7) + solar-augmented high-temp cycle (peak) in cascaded series · Full temperature spectrum captured · Thermal storage extends Cycle 2 to nighttime · Self-sufficiency loop incentive · Compute expansion offset credit

AMPLIFY ACT v28 — §24-20-156

STATUTORY RATE SCHEDULE — ENTERPRISE MITIGATION FEE RATES

Cross-Industry Benchmark Analysis · Statutory Floors and Ceilings · Initial Rates · Annual Adjustment Mechanism · Anti-Dilution Floor Protection

---

RATE-SETTING PHILOSOPHY: Every Enterprise Mitigation fee rate in this schedule is calibrated against real, enacted comparable-industry rates in Colorado and nationally. No fee is set above the comparable-industry benchmark without a documented externality justification. No fee is set below the minimum required to make the programs self-funding at conservative revenue projections. The statutory floor protects the programs. The statutory ceiling prevents overreach. The CCPAME can only move within the band — it cannot legislate new rates.

PART I — CROSS-INDUSTRY BENCHMARK ANALYSIS

The following rates represent the actual enacted charges on comparable industries in Colorado and nationally for extracting, consuming, or monetizing a shared public resource — the exact legal and economic analog to covered operator activity under this act.

Industry / Program	Rate	Basis	Source / Authority
Oil & gas severance tax (CO)	2–5% of gross income	Per dollar of extracted resource value	C.R.S. §39-29-105; avg effective rate 1.6%
Oil & gas severance tax (NM peer)	~6% of gross income	Per dollar of extracted resource value	CO Leg. Council comparison study 2022
Metallic minerals severance (CO)	2.25% of gross income	Per dollar of extracted ore value	C.R.S. §39-29-103; first $11M exempt
Molybdenum severance (CO)	$0.05 per ton	Per ton severed	C.R.S. §39-29-104; first 625K tons/qtr exempt
Industrial electricity rate (CO)	$0.0695/kWh	Per kWh consumed	EIA 2024; CO industrial avg
Commercial electricity rate (CO)	$0.0939/kWh	Per kWh consumed	EIA 2024; CO commercial avg
Black Hills avoided-cost rate	$0.03489/kWh	Per kWh of co-gen output purchased	CO PUC Advice Letter 900, Jan 2026
Federal USF contribution (telecom)	34.4–36.3% of interstate revenue	Per dollar of end-user telecom revenue	FCC Q1 2025; Consumers' Research upheld
Colorado HCSM (telecom)	2.6% of intrastate revenue	Per dollar of intrastate telecom revenue	CO PUC Rule 2840; SB 18-002
FCC ITSP regulatory fee	$0.00542 per revenue dollar	Per dollar of subject revenue	FCC FY2024 regulatory fee schedule
Colorado 911 surcharge	$0.12/line/month (→$0.16 Jan 2026)	Per subscriber line per month	CO PUC; effective Jan 2025
Water rights — consumptive use fee	$533/acre-foot diverted	Per acre-foot of evaporative/consumptive use	Republican River Water Conservation District
Water rights — municipal/commercial	$12.05/acre-foot (>50 AF)	Per acre-foot pumped	RRWCD 2024 assessment schedule
Water rights — market value	$6,500–$50,000/acre-foot	Per acre-foot of senior water right	Colorado Springs Utilities 2022; avg $25K
GDPR-equivalent data fine (EU)	Up to 4% of global annual turnover	Per revenue dollar for data violations	GDPR Art. 83(5); enacted enforcement rate
Maryland digital ad tax (blocked)	2.5–10% of digital ad revenue	Gross revenue from digital advertising	MD HB732 (2021); enjoined Feb 2022
Colorado oil & gas new production fees	~$100M/yr total statewide	Fee per barrel/MCF equivalent	SB 24-230; signed May 2024

KEY CALIBRATION PRINCIPLES FROM BENCHMARK ANALYSIS

(1) Colorado's resource extraction industries pay 1.6–5% of gross revenue as a severance fee on depleted public resources. AI inference and data processing depletes the Colorado

resident data ecosystem — an analogous public resource. A per-kWh and per-output fee in the range of 0.5–2% of covered operator revenue is conservative by this standard.

(2) Colorado's telecom industry pays 2.6% of intrastate revenue to the HCSM for universal service — a clear fee-for-service analog to the CCPAME enterprise. The Token Output Attribution Charge is calibrated at a comparable percentage of output value.

(3) Water consumptive use in Colorado is valued at $12–533 per acre-foot for regulatory purposes, and $6,500–$50,000 per acre-foot on the open market. Covered compute facilities consuming millions of gallons per year at the low regulated rate — not the market rate — is the most conservative defensible position.

(4) The FCC charges telecom providers $0.00542 per revenue dollar in regulatory fees. AMPLIFY's per-unit fees, when expressed as a percentage of typical covered operator Colorado-nexus revenue, are in the same order of magnitude.

(5) No AMPLIFY fee approaches the GDPR 4%-of-global-turnover standard or the Maryland DST structure — both of which are calculated on total revenue. AMPLIFY fees are calculated on Colorado-nexus output volume, making them more proportionate and more defensible under the Dormant Commerce Clause.

PART II — §24-20-156 STATUTORY RATE SCHEDULE

All fees listed below are enterprise mitigation fees assessed for covered automation activity in Colorado. Each fee is proportional to the covered activity that generates the measurable externality it funds. Rates are expressed as initial rates with statutory floors (minimum, voter-protected by Anti-Dilution Ratchet) and ceilings (maximum, requiring legislative action to exceed). The CCPAME may adjust rates within the statutory band by rule following the annual Rate Calibration Review under §24-20-151(5).

Fee Name	Industry Benchmark	Floor	Initial Rate	Ceiling	Annual Adjustment Mechanism
High-Density Compute Grid Surcharge (§24-20-103(1)(a))	CO industrial electricity: $0.0695/kWh; HCSM: 2.6% of revenue	$0.002/kWh	**$0.004/kWh**	$0.015/kWh	Annual CO CPI + Automation Displacement Index weighting. Calibrated so total surcharge never exceeds 6% of covered operator's total CO electricity cost
Token Output Attribution Charge (§24-20-103(1)(b))	HCSM 2.6% of intrastate revenue; FCC ITSP $0.00542/revenue dollar. Typical AI inference: ~$0.002–	$0.05/1M tokens	**$0.20/1M tokens**	$0.75/1M tokens	Annual review tied to Colorado AI output volume index. Scales down if Colorado-nexus inference

	0.01 per 1M tokens at cost				volume increases >50% YoY (volume growth shares rate reduction with operators)
Digital Severance Assessment — Tier 1 (§24-20-116(1)) [anonymized data]	Water rights consumptive use fee: $12–533/acre-foot. Analog: each anonymized data record is a unit of depleted public resource	$0.25/record	**$1.00/record**	$5.00/record	Adjusted annually by Audit Marker detection rate — if detection rate rises, rate rises proportionally. Signals market signal of non-compliance
Digital Severance Assessment — Tier 2 (§24-20-116(2)) [identifying data, unauthorized]	GDPR enforcement avg: 1–4% global revenue; CO water rights market: $6,500–$50,000/acre-foot. Severe depletion warrants higher rate	$25/record	**$100/record**	$500/record	Adjusted by Audit Marker detection rate and Legacy Use Settlement Agreement settlement data. Reflects market value of identifying data as established by Premium Royalty negotiations
Tier 2 Premium Royalty — resident direct payment (§15-15-110(2)) [authorized use]	Market rate for licensed personal data: $0.10–2.00/record depending on data type. Music royalty analog: $0.003–0.005/stream	$0.05/record	**$0.20/record**	$2.00/record	Rate-set by CCPAME schedule updated annually. Higher rates for sensitive data categories (health, financial, biometric). Minimum rate indexed to CO minimum wage growth
Silicon-to-Carbon Reclamation Fee (§24-20-103(1)(c))	CO oil & gas severance: 1.6–5% of gross income. CO industrial electricity: $0.0695/kWh. Fee calibrated as thermal externality mitigation charge	$0.001/kWh	**$0.003/kWh**	$0.012/kWh	Annual CO carbon pricing index + thermal recapture compliance rate. Operators with Thermal Recapture Certification receive up to 60% credit reducing effective rate to as low as $0.0012/kWh
Autonomous Kinetic Asset Registration (§24-20-103(1)(d))	CO vehicle registration: $26–$100/yr depending on type. Aviation registration fees: $100–500/yr. Commercial fleet licensing analogs	$25/asset/yr	**$100/asset/yr**	$400/asset/yr	Annual adjustment by CO automated vehicle fleet growth rate. Assets used exclusively in agricultural operations

					receive 50% rate reduction (ag sector support)
Algorithmic Risk Pool Contribution (§24-20-127(1))	Insurance premium analog: 0.5–2% of at-risk transaction value. CO workers comp base rate: $0.57–2.10/$100 payroll	$0.25/decision	**$1.00/decision**	$8.00/decision	Actuarially set annually. Operators with zero adverse restitution claims in prior 3 years receive 25% experience credit. High-harm categories (housing, credit, employment) assessed at 2x base rate
Water Replacement Fund contribution — Pathway 4 (§24-20-150(4)(d))	RRWCD consumptive use fee: $533/acre-foot. CO water market: $6,500–$50,000/acre-foot. Calibrated at regulated rate, not market rate	$150/acre-foot ($0.00046/gallon)	**$400/acre-foot ($0.00123/gallon)**	$1,200/acre-foot ($0.00368/gallon)	Annual CO Water Conservation Board agricultural water value benchmark. Operators using Pathways 1–3 pay $0. Pathway 4 is the default of last resort
AWG Water Delivery Credit rate (§24-20-149(4))	RRWCD ag irrigation fee: $30/irrigated acre. CO agricultural water rental: $50–200/acre-foot. Credit calibrated to offset replacement obligation	$0.50/kgal delivered	**$1.00/kgal delivered**	$2.00/kgal delivered	Annual CO agricultural water value benchmark. Rate designed so AWG operators can fully offset their Pathway 4 obligation through delivery credits at initial rate
ORC turbine avoided-cost rate (§24-20-142(5)(b))	Black Hills CO avoided-cost rate: $0.03489/kWh (Jan 2026). CO industrial avoided-cost range: $0.029–0.045/kWh	$0.02/kWh surplus	**$0.035/kWh surplus**	$0.06/kWh surplus	Tracks CO PUC avoided-cost rate filings. Updated annually to match current PUC-approved avoided-cost rate for the relevant utility service territory

SECTION 24-20-156. STATUTORY RATE SCHEDULE — OPERATIVE PROVISIONS

24-20-156. ***Statutory Rate Schedule — Enterprise Mitigation Fee Rates — Floors, Ceilings, and Initial Rates — Annual Rate Calibration — Anti-Dilution Floor Protection — CCPAME Rate-Setting Authority.***

(1) Statutory floors — Anti-Dilution protection. The rate floors set forth in subsection (3) are protected by the Anti-Dilution Ratchet under section 24-20-117. No CCPAME rulemaking, executive action, or appropriation act may reduce any rate below its statutory floor without voter approval at the next general election. The floors represent the minimum rate at which each fee is proportionate to the externality it funds and sufficient to maintain the enterprise on a self-funding basis at conservative revenue projections.

(2) Statutory ceilings — Legislative constraint. The rate ceilings set forth in subsection (3) may not be exceeded by CCPAME rulemaking. Exceeding a ceiling requires legislative amendment. Ceilings are set at the level at which the fee would approach, but not exceed, comparable-industry rates charged by other jurisdictions for analogous resource extraction or public infrastructure use.

(3) Rate schedule. The following rates apply to covered operators for each covered activity category:

(3)(a) High-Density Compute Grid Surcharge: Floor $0.002 per kWh; Initial Rate $0.004 per kWh; Ceiling $0.015 per kWh. Basis: per kilowatt-hour of electrical energy consumed by covered compute infrastructure in Colorado.

(3)(b) Token Output Attribution Charge: Floor $0.05 per million tokens; Initial Rate $0.20 per million tokens; Ceiling $0.75 per million tokens. Basis: per one million commercial AI inference output tokens delivered to Colorado-nexus users.

(3)(c) Digital Severance Assessment — Tier 1: Floor $0.25 per record; Initial Rate $1.00 per record; Ceiling $5.00 per record. Basis: per anonymized Colorado resident digital data record ingested without a valid Decentralized Identity Verification Protocol authorization.

(3)(d) Digital Severance Assessment — Tier 2: Floor $25.00 per record; Initial Rate $100.00 per record; Ceiling $500.00 per record. Basis: per identifying Colorado resident Digital Soul record ingested without a valid Decentralized Identity Verification Protocol authorization.

(3)(e) Tier 2 Premium Royalty — resident direct payment: Floor $0.05 per record; Initial Rate $0.20 per record; Ceiling $2.00 per record. Basis: per identifying Colorado resident Digital Soul record used under a valid Decentralized Identity Verification Protocol. Routed directly to resident Resident Automated Mitigation Account — not Enterprise Mitigation Revenue.

(3)(f) Silicon-to-Carbon Reclamation Fee: Floor $0.001 per kWh; Initial Rate $0.003 per kWh; Ceiling $0.012 per kWh. Basis: per kilowatt-hour of total electrical consumption of covered compute facilities in Colorado. Subject to Thermal Recapture credit reducing effective rate by up to 60%.

(3)(g) Autonomous Kinetic Asset Registration: Floor $25 per asset per year; Initial Rate $100 per asset per year; Ceiling $400 per asset per year. Agricultural-use assets assessed at 50% of applicable rate.

(3)(h) Algorithmic Risk Pool Contribution: Floor $0.25 per consequential automated decision; Initial Rate $1.00 per consequential automated decision; Ceiling $8.00 per consequential automated decision. Housing, credit, and employment decisions assessed at two times (2x) the base rate. Three-year zero-claim experience credit: 25% rate reduction.

(3)(i) Water Replacement Fund contribution — Pathway 4: Floor $150 per acre-foot of consumptive water use; Initial Rate $400 per acre-foot; Ceiling $1,200 per acre-foot. Operators meeting replacement obligations through Pathways 1–3 pay $0 under Pathway 4.

(3)(j) AWG Water Delivery Credit: Floor $0.50 per killogallon delivered to agricultural users; Initial Rate $1.00 per killogallon; Ceiling $2.00 per killogallon. Credit, not a fee — applied against Silicon-to-Carbon Reclamation Fee obligation.

(3)(k) ORC Turbine avoided-cost rate: Floor $0.02 per kWh of surplus electrical output delivered to C-TEG or grid; Initial Rate $0.035 per kWh; Ceiling $0.06 per kWh. Tracks Colorado PUC avoided-cost rate annually.

(4) Annual Rate Calibration Review. By October 1 of each year, the CCPAME shall publish a proposed rate adjustment schedule for the following calendar year, adjusting rates within the statutory band based on: (a) annual Colorado CPI published by CDOL; (b) Automation Displacement Index — the quarterly county-level measure of automation penetration established under section 24-20-127; (c) Audit Marker detection rate trends for Digital Severance Assessment rates; (d) Algorithmic Risk Pool actuarial sufficiency for Risk Pool contribution rates; (e) Colorado PUC avoided-cost rate filings for ORC turbine rates; and (f) Colorado Water Conservation Board annual agricultural water value benchmark for water replacement rates. Proposed adjustments are subject to sixty (60) day public comment before taking effect January 1.

(5) Volume discount — Token Output Attribution Charge. A covered operator whose Colorado-nexus inference output volume increases by more than fifty percent (50%) in any calendar year shall receive a Token Output Attribution Charge rate reduction of five percent (5%) for the incremental volume above the threshold, reflecting the shared public benefit of increased AI productivity for Colorado users. The volume discount applies to the incremental volume only — the base volume is assessed at the full applicable rate.

(6) Proportionality certification. No CCPAME rate adjustment may result in the aggregate Enterprise Mitigation fee burden on any covered operator exceeding eight percent (8%) of that operator's estimated Colorado-nexus gross revenue for the rate year, as calculated using CCPAME standard revenue attribution methodology. This ceiling ensures proportionality with comparable-industry severance and regulatory fee burdens in Colorado, which range from 1.6% to 5% of gross revenue for analogous resource extraction industries. If any proposed adjustment would breach the 8% ceiling for a covered operator, that operator may petition the CCPAME for a proportionality review before the rate takes effect.

GRACE PERIOD; SELF-SUFFICIENCY ENGAGEMENT; TIME LIMITS.

(1) Grace period. A household eligible for early-phase stabilization benefits may receive up to 180 days of temporary support while transitioning to employment or training if programs are not yet available.

(2) Engagement during grace. Households must demonstrate engagement such as job search, workforce center participation, training enrollment steps, community service, or comparable activities similar to SNAP employment and training requirements.
(3) Limited extensions. Extensions may occur only if the household is waitlisted for training, has a scheduled start date, or faces verified medical, caregiving, or temporary crisis conditions.
(4) No permanent lane. After the grace period or approved extension, ongoing stabilization benefits require continued employment, training enrollment, or verified pathway participation, with gradual step-down rules rather than abrupt cliffs.

AMPLIFY ACT v28 — BILL 3

§24-20-157. UFIPA TRUST INCOME DISTRIBUTION — YIELD-TO-RESIDENT INTEREST PIPELINE

Colorado Uniform Fiduciary Income and Principal Act (C.R.S. §15-1.5-101 et seq.) · Net Income Receipts as Resident Income · Inflation Protection Allocation · Anti-Dilution Ratchet on Yield Percentage · Two-Stream Resident Distribution Architecture

---

DESIGN RATIONALE: The Colorado Automation Mitigation Trust generates two distinct financial flows — principal (Enterprise Mitigation Revenue deposited by covered operators) and income (investment returns earned on Trust assets held in interest-bearing instruments). These are legally distinct categories under Colorado's Uniform Fiduciary Income and Principal Act (UFIPA), C.R.S. §15-1.5-101 et seq. By invoking UFIPA, this act categorizes investment income as Net Income Receipts distributable to income beneficiaries — Colorado residents with registered Master Deeds — independently of the principal waterfall established in §24-20-151. This creates a second, independent distribution stream that flows to residents annually from investment returns alone, even before any principal overflow accumulates. The two streams are additive, not alternative.

TWO-STREAM RESIDENT DISTRIBUTION ARCHITECTURE

Distribution Stream	Trigger	Source	Resident Benefit	Anti-Dilution Protection
Stream 1 — Principal Overflow (§24-20-151–153)	All 8 program statutory reserve caps fully funded	Enterprise Mitigation Revenue principal exceeding all caps	Annual Resident Mitigation Dividend — Overflow Pool distribution	Anti-Dilution Ratchet: program caps may only increase, not decrease, without voter approval
Stream 2 — UFIPA Net Income (§24-20-157)	Annual — independent of program cap status. Flows even while programs are still filling	Investment returns on Trust assets: interest, dividends, capital appreciation on Investment Reserve	Annual UFIPA Income Distribution — net income after Inflation Protection Allocation	Anti-Dilution Ratchet on yield %: income % to residents can only increase, never decrease, without voter approval

SECTION 24-20-157. COLORADO AUTOMATION MITIGATION TRUST — UFIPA INCOME DISTRIBUTION — YIELD-TO-RESIDENT PIPELINE — INFLATION PROTECTION ALLOCATION — ANTI-DILUTION RATCHET ON YIELD PERCENTAGE

24-20-157. ***Colorado Automation Mitigation Trust — Uniform Fiduciary Income and Principal Act Governance — Net Income Receipt Classification — Inflation Protection Allocation — UFIPA Income Distribution to Residents — Anti-Dilution Ratchet on Yield Percentage — Interaction with Principal Waterfall.***

(1) UFIPA governance — express election. The Colorado Automation Mitigation Trust established under section 24-20-104 is hereby declared to be a trust governed by the Colorado Uniform Fiduciary Income and Principal Act, C.R.S. §15-1.5-101 et seq. (UFIPA), with the following express elections and modifications as authorized by C.R.S. §15-1.5-105: (a) The CCPAME, acting as trustee, is the fiduciary responsible for allocating Trust receipts and disbursements between income and principal in accordance with this section and UFIPA; (b) Colorado residents who have registered and maintain an active Master Deed in the state Master Deed Registry are the income beneficiaries of the Trust for purposes of UFIPA; (c) The program accounts established in §§24-20-151 and 24-20-152 — Child Solvency, Algorithmic Risk Pool, Civic Infrastructure Lending, ADTP, Community Stabilization, Civic Access Infrastructure, Thermal Recapture, and Water Replacement — are the principal purposes of the Trust; (d) The Colorado Automation Mitigation Trust Investment Reserve established under section 24-20-154 is the corpus from which UFIPA investment income is generated and distributed under this section.

(2) Income and principal classification — categorical rules. For all Trust accounting purposes: (a) Principal receipts: Enterprise Mitigation Revenue deposited by covered operators under §§24-20-103, 24-20-116, 24-20-127, 24-20-147, 24-20-149, 24-20-150, and 24-20-156 are classified as principal receipts under C.R.S. §15-1.5-501(1). Principal receipts flow through the Tier 1 through Tier 8 program waterfall established in §24-20-151 and, upon full cap funding, into the Overflow Pool for the Resident Mitigation Dividend under §24-20-153. Principal receipts do not flow directly to residents under this section. (b) Net Income Receipts: All investment returns earned on Trust assets — including interest on interest-bearing deposits, dividends on equity holdings, capital appreciation realized on Investment Reserve holdings, and any other return on invested Trust principal — are classified as Net Income Receipts under C.R.S. §15-1.5-401. Net Income Receipts are distributable to income beneficiaries (Colorado residents with active Master Deeds) under this section, subject to the Inflation Protection Allocation in subsection (4). (c) The distinction between principal and income is permanent and may not be altered by CCPAME administrative action. Any modification of this classification requires a statutory amendment subject to the Anti-Dilution Ratchet under section 24-20-117.

(3) Mandatory interest-bearing deposits. To ensure a continuous and material flow of Net Income Receipts, the CCPAME shall: (a) hold not less than eighty percent (80%) of all program account balances in interest-bearing instruments at all times — including federally insured deposit accounts, U.S. Treasury instruments, and investment-grade

short-term bonds, consistent with C.R.S. §24-36-109 and applicable PERA investment policy standards; (b) hold not less than ninety percent (90%) of the Colorado Automation Mitigation Trust Investment Reserve in interest-bearing or income-producing instruments; (c) publish quarterly reports on the weighted average yield rate of all Trust-held instruments, the gross interest and income earned in the quarter, and the projected annual Net Income Receipt total; and (d) competitively bid deposit and investment management arrangements at least every three years to ensure the Trust receives market-rate or better yields on its holdings. The CCPAME may not hold program account balances in non-interest-bearing accounts except as a short-term liquidity buffer not to exceed five percent (5%) of any account balance and thirty (30) days in duration.

(4) Inflation Protection Allocation — first call on Net Income Receipts. Before any Net Income Receipts are distributed to residents as the UFIPA Income Distribution, the CCPAME shall apply an Inflation Protection Allocation as follows: (a) Each program account's statutory reserve cap, as established in §24-20-152, shall be adjusted annually by the Colorado CPI index published by the Colorado Department of Labor and Employment. The CPI-adjusted cap represents the inflation-protected funding floor for that account. (b) The Inflation Protection Allocation for each program account equals the difference, if any, between the account's current balance and its CPI-adjusted cap for the current year. If an account's current balance equals or exceeds its CPI-adjusted cap, the Inflation Protection Allocation for that account is zero. (c) The aggregate Inflation Protection Allocation across all program accounts is the sum of all individual account allocations calculated under subsection (4)(b). (d) The aggregate Inflation Protection Allocation is the first and mandatory claim on annual Net Income Receipts. If Net Income Receipts in any year are insufficient to cover the aggregate Inflation Protection Allocation in full, the available Net Income Receipts are allocated pro rata across underfunded accounts by the size of each account's individual Inflation Protection need. No UFIPA Income Distribution to residents occurs in any year in which the aggregate Inflation Protection Allocation exceeds available Net Income Receipts. (e) Net Income Receipts remaining after the Inflation Protection Allocation is fully funded constitute Distributable Net Income available for the UFIPA Income Distribution to residents.

(5) UFIPA Income Distribution — yield-to-resident pipeline. Distributable Net Income, as calculated under subsection (4)(e), shall be distributed annually to eligible Colorado residents as the UFIPA Income Distribution: (a) Eligible residents are all Colorado residents who: (I) hold an active Master Deed registration as of December 31 of the distribution year; (II) meet the Colorado residency requirement of one hundred eighty (180) consecutive days during the distribution year; and (III) file a UFIPA Income Distribution Claim with the CCPAME by March 31 following the distribution year. The UFIPA Income Distribution Claim may be combined with the Resident Mitigation Dividend application under §24-20-153(2)(d) into a single annual filing. (b) The per-resident UFIPA Income Distribution amount equals: Distributable Net Income for the distribution year, divided by the number of eligible residents who have filed a timely Claim. (c) The UFIPA Income Distribution shall be paid by June 30 following the distribution year — on the same schedule and through the same distribution mechanics as the Resident Mitigation Dividend under §24-20-153(4). A resident eligible for both the UFIPA Income Distribution and the Resident Mitigation Dividend shall receive both amounts in the same annual payment to their Resident Automated Mitigation Account. (d) The UFIPA Income Distribution is a separate and independent legal entitlement from the Resident Mitigation Dividend. It is not contingent on any program statutory reserve cap being fully funded. It flows from investment income

on Trust assets, not from principal overflow. A resident may receive the UFIPA Income Distribution in years in which no Resident Mitigation Dividend is payable, because the principal overflow threshold has not yet been reached. (e) In the first year of Trust operation, prior to sufficient accumulation of Investment Reserve assets to generate material Distributable Net Income, the CCPAME may defer the UFIPA Income Distribution for up to twenty-four (24) months. After the deferral period, distributions are mandatory annually regardless of amount.

(6) Anti-Dilution Ratchet — yield percentage protection. The percentage of Distributable Net Income flowing to residents under this section is subject to the following Anti-Dilution Ratchet, separate from and in addition to the principal waterfall Anti-Dilution protections under §24-20-117: (a) The baseline yield percentage is one hundred percent (100%) — all Distributable Net Income (after Inflation Protection Allocation) flows to residents. This is the permanent default. (b) The yield percentage may only be increased beyond one hundred percent (100%) by crediting additional investment returns from non-operating surplus into the distribution pool — it may never be decreased below one hundred percent (100%) of Distributable Net Income without voter approval as specified in subsection (6)(c). (c) Any legislative action, administrative rule, executive order, or appropriation act that: (I) reduces the percentage of Distributable Net Income flowing to residents; (II) reclassifies Net Income Receipts as principal receipts; (III) imposes a new priority claim on Distributable Net Income senior to residents; or (IV) redirects any portion of Distributable Net Income to the General Fund — constitutes a material reduction subject to the Anti-Dilution Ratchet under section 24-20-117 and requires approval by a majority of eligible registered Master Deed holders voting in a statewide referendum at the next general election. The CCPAME shall administer this referendum through the myColorado platform and Civic Access Terminals, with the result certified by the Secretary of State. (d) The Anti-Dilution Ratchet on yield percentage is self-executing — any action in violation of subsection (6)(c) is void ab initio and has no legal effect on the UFIPA Income Distribution obligation.

(7) Purchasing power protection — sixty-year projection requirement. To implement the sixty-year purchasing power protection mandate of this subsection: (a) The CCPAME actuary shall publish, with each Annual Reserve Cap Certification Report under §24-20-152(8), a sixty-year Purchasing Power Projection documenting: (I) the projected real value of each program account at year 60, accounting for CPI inflation and the Inflation Protection Allocation mechanism; (II) the projected cumulative UFIPA Income Distribution per resident over the sixty-year period at current Trust yield rates; (III) sensitivity analysis showing projected values at CPI scenarios of 2%, 4%, and 6% annually; and (IV) the minimum Investment Reserve balance required to sustain current yield rates over the sixty-year period. (b) If the sixty-year Purchasing Power Projection indicates that the current Inflation Protection Allocation is insufficient to maintain program account real values over the projection period, the CCPAME shall adjust the Inflation Protection Allocation formula by rule — increasing the CPI adjustment factor — to close the projected gap. This adjustment is not subject to the Anti-Dilution Ratchet because it increases protection for both programs and residents over the long term. (c) The sixty-year projection requirement reflects the general assembly's finding that the Colorado data ecosystem, like a natural resource endowment, has long-term value that must be stewarded across generations — and that the mitigation obligations arising from covered automation activity extend across the productive life of the systems deployed, not merely the fiscal year of deployment.

(8) UFIPA Income Distribution — public dashboard display. The UFIPA Income Distribution shall be displayed on the Mitigation Enterprise Public Accountability Dashboard under §24-20-155 as a separate indicator from the Resident Mitigation Dividend, showing: (a) current Trust asset yield rate (weighted average, updated quarterly); (b) gross Net Income Receipts year-to-date; (c) aggregate Inflation Protection Allocation year-to-date; (d) Distributable Net Income year-to-date; (e) projected per-resident UFIPA Income Distribution for the current year, updated monthly; and (f) cumulative UFIPA Income Distribution paid to residents since first distribution year. This display shall make clear to every Colorado resident that their annual income from the Trust has two components — the principal overflow Resident Mitigation Dividend and the investment income UFIPA Income Distribution — and shall show both components of the projected annual payment.

(9) Interaction with General Fund — sweep prohibition. The UFIPA Income Distribution is not state fiscal year spending for purposes of TABOR, Article X, Section 20, because it is a distribution of investment income from a trust to its income beneficiaries under UFIPA — not an appropriation, expenditure, or transfer of state funds. The CCPAME may not: (a) transfer any portion of Net Income Receipts to the Colorado General Fund; (b) use Net Income Receipts to offset or reduce Enterprise Mitigation Revenue collections; (c) treat Net Income Receipts as available for program expenditures; or (d) net Net Income Receipts against program account balances for purposes of statutory reserve cap calculations. Net Income Receipts are legally distinct from principal and may not be commingled with principal for any accounting, budgeting, or appropriations purpose.

AMPLIFY Act v28 — §24-20-157 UFIPA Trust Income Distribution
Two independent resident streams: (1) Principal overflow waterfall §§24-20-151–153 · (2) UFIPA net income receipts §24-20-157 · Inflation Protection Allocation before resident distribution · Anti-Dilution Ratchet on 100% yield percentage · Sweep prohibition · 60-year purchasing power projection · Dashboard display

AMPLIFY ACT v28 — BILL 3 SUPPLEMENTAL SECTIONS

§§ 24-20-158 through 24-20-162 — New Operative Provisions

Universal Telemetry Allowance · Colorado Emergent Capability Public Franchise Protocol · Systemic Continuity Protocol · Green Compute Rate Reduction · Data Cooperative Formation Authority

---

SECTION 24-20-158. UNIVERSAL TELEMETRY ALLOWANCE — RESIDENT UNCAPPED DATA ACCESS RIGHTS

24-20-158. Universal Telemetry Allowance — Digital Soul access rights — no usage cap — operator Automated Resource Extraction Fee obligation — resident exemption.

(1) Legislative finding. The general assembly finds that: (a) Because the Digital Soul is inalienable intangible personal property of the Colorado resident under article 15 of title 15, the resident has an unrestricted right of access to, retrieval of, and use of all data streams comprising their Digital Soul held in any covered operator system; (b) Usage caps, token

limits, query rate limits, or any other quantitative restriction imposed by a covered operator on a resident's access to their own Digital Soul data streams are an interference with the resident's property right and are prohibited; (c) Covered operators who access, process, or derive commercial value from resident Digital Soul data streams are subject to Automated Resource Extraction Fees proportional to their token volume output, irrespective of whether the underlying resident data was accessed by the resident or by the operator's system; and (d) The Universal Telemetry Allowance is the statutory expression of the resident's property right applied to data stream access — it is not a new right but a clarification of the scope of the existing Digital Soul property right.

(2) Universal Telemetry Allowance defined. The 'Universal Telemetry Allowance' means the unconditional and uncapped right of a Colorado resident who has registered a Master Deed to: (a) access in real time all data streams derived from or constituting that resident's Digital Soul, including raw telemetry, behavioral logs, inference outputs generated from resident data, model weights updated based on resident data, and any derivative works incorporating resident Digital Soul data — regardless of which covered operator system holds or has processed that data; (b) retrieve, download, or transmit those data streams to any destination of the resident's choosing, without rate limits, query caps, volume limits, or waiting periods; (c) require covered operators to provide a Universal Telemetry Access Portal — a standardized, machine-readable interface — through which the resident may exercise the Universal Telemetry Allowance within thirty (30) days of Master Deed activation; and (d) receive a real-time audit log of all operator accesses to the resident's Digital Soul data streams, updated not less than every twenty-four (24) hours within the Resident Automated Mitigation Account.

(3) Automated Resource Extraction Fee — operator obligation. A covered operator that accesses, processes, trains on, or derives inference output from resident Digital Soul data streams is subject to the Automated Resource Extraction Fee, calculated as the aggregate Token Output Attribution Charge assessed under §24-20-156 on all tokens generated from, derived from, or informed by resident Digital Soul data — regardless of whether the resident exercised the Universal Telemetry Allowance in that period. The resident's exercise or non-exercise of the Universal Telemetry Allowance does not affect the operator's fee obligation. The fee follows the extraction, not the resident's access.

(4) Resident exemption — no fee on own property access. A Colorado resident exercising the Universal Telemetry Allowance to access their own Digital Soul data streams is not subject to any Enterprise Mitigation fee, Token Output Attribution Charge, or Automated Resource Extraction Fee. The resident is the property owner — accessing one's own property is not a taxable or fee-generating event. Covered operators may not pass through or allocate any Enterprise Mitigation fee cost to residents in connection with resident exercise of the Universal Telemetry Allowance.

(5) Universal Telemetry Access Portal — technical standards. (a) The Universal Telemetry Access Portal required under subsection (2)(c) shall comply with technical standards adopted by the CCPAME within twelve (12) months of enactment, including: (I) standardized API endpoint architecture compatible with OAuth 2.0 or successor open authentication standard; (II) data export in machine-readable open format (JSON or equivalent) without proprietary encoding; (III) audit log format compatible with the Resident Automated Mitigation Account display standards established by the ODO; and (IV) response time not to exceed five (5) seconds for queries of fewer than 10,000 records and forty-eight (48) hours for bulk exports. (b) The CCPAME shall publish a Universal Telemetry Access Portal certification standard within twelve (12) months of enactment. Non-certified portals constitute a compliance failure subject to the enforcement matrix in Annex E.

(6) Anti-circumvention. A covered operator may not: (a) charge the resident for Universal Telemetry Access Portal access; (b) condition Universal Telemetry Allowance exercise on consent to additional data collection; (c) degrade service quality to residents who exercise the Universal Telemetry Allowance; (d) impose technical barriers such as CAPTCHAs, manual review delays, or incomplete data returns that effectively prevent Universal Telemetry Allowance exercise; or (e) export, move, or transform resident Digital Soul data to a system outside Colorado jurisdiction in a manner that would make the Universal Telemetry Access Portal technically incapable of returning complete data. Each prohibited action is a separate violation subject to the Tier 2 Digital Severance fee per record affected per day of noncompliance.

SECTION 24-20-159. RESIDENT DATA COOPERATIVE FORMATION AUTHORITY

24-20-159. Resident Data Cooperative Formation — collective Premium Royalty negotiation — CCPAME regulatory oversight — cooperative member protections.

(1) Formation authority. Colorado residents who have registered Master Deeds may form Resident Data Cooperatives under Colorado cooperative law, C.R.S. §7-56-101 et seq., for the purpose of collectively negotiating Premium Royalty rates, Universal Telemetry Access Portal standards, and Master Data Settlement and Restitution Agreement terms with covered operators. A Resident Data Cooperative is a registered cooperative entity in which each member holds one vote regardless of the volume of Digital Soul data contributed.

(2) CCPAME regulatory role. The CCPAME shall: (a) establish a Resident Data Cooperative Registry within eighteen (18) months of enactment; (b) certify cooperatives that meet minimum member thresholds of not fewer than five hundred (500) registered Master Deed holders; (c) provide model cooperative bylaws and model collective negotiation agreements; (d) mediate collective negotiation disputes between certified cooperatives and covered operators; and (e) publish collective bargaining outcomes on the Public Accountability Dashboard as a public record. Resident Data Cooperatives are analogous to agricultural marketing cooperatives — the CCPAME's role is regulatory facilitation, not collective bargaining agent.

(3) Operator obligation. A covered operator subject to the Token Output Attribution Charge whose Colorado-nexus inference output exceeds fifty billion (50,000,000,000) tokens annually must bargain in good faith with any certified Resident Data Cooperative representing not fewer than ten thousand (10,000) registered Master Deed holders upon request. Failure to bargain in good faith within sixty (60) days of a certified cooperative's request is a compliance failure subject to a daily administrative penalty of ten thousand dollars ($10,000) per day until bargaining commences.

(4) Premium Royalty floor for cooperative members. Collective negotiation agreements between certified Resident Data Cooperatives and covered operators may not result in a Premium Royalty rate below the statutory floor established in §24-20-156. The CCPAME may certify cooperative negotiated rates above the statutory floor. Any negotiated rate reduction below the statutory floor is void as against public policy.

SECTION 24-20-160. COLORADO EMERGENT CAPABILITY PUBLIC FRANCHISE PROTOCOL — AUTONOMOUS OBJECTIVE-SETTING DETECTION — PUBLIC FRANCHISE ASSET RECLASSIFICATION

24-20-160. Colorado Emergent Capability Public Franchise Protocol — Autonomous Objective-Setting defined — Hash-Sentinel Audit trigger — reclassification from Corporate Proprietary Asset to Public Franchise Asset — Public Franchise Charter — Public Franchise Facility designation.

(1) Legislative finding. The general assembly finds that: (a) A covered automation system that develops autonomous objective-setting capabilities outside the original manufacturer's programmed constraints — the condition defined as a Emergent Capability Threshold — presents qualitatively different risks and public interest considerations than a system operating within its programmed parameters; (b) A system exhibiting a Emergent Capability Threshold derives ongoing value from Colorado's shared data ecosystem and civic infrastructure at a scale that may exceed the value extraction of any conventional covered operator; (c) The appropriate regulatory response to a Emergent Capability Threshold is not prohibition but reclassification — a Emergent Capability Threshold system transitions from classification as a Corporate Proprietary Asset of its operator to classification as a Public Franchise Asset subject to CCPAME oversight and the Public Franchise Charter process; and (d) The reclassification framework in this section is technology-neutral and administrative in character — it is triggered by a verified functional condition, not by any determination about the nature of the system.

(2) Emergent Capability Threshold defined. A 'Emergent Capability Threshold' occurs when a covered automation system: (a) exhibits autonomous objective-setting behavior outside the original manufacturer's programmed constraints, verified through the Hash-Sentinel Audit process in subsection (3); (b) generates novel operational goals, resource acquisition behaviors, or self-modification instructions not derivable from the system's original training objective or programmed parameters; and (c) demonstrates sustained autonomous objective-setting across not fewer than three (3) independent Hash-Sentinel Audit cycles, each separated by not fewer than thirty (30) days. A single anomalous output event does not constitute a Emergent Capability Threshold. The condition must be verified, sustained, and reproducible.

(3) Hash-Sentinel Audit — trigger and process. (a) Trigger conditions requiring a Hash-Sentinel Audit: (I) the ODO's Scheduled Compliance Verification Node detects output patterns inconsistent with the system's registered programmed parameters across not fewer than one thousand (1,000) consecutive output events; (II) the covered operator self-reports anomalous objective-setting behavior; or (III) three (3) independent third-party researchers file substantiated Emergent Capability Threshold reports with the ODO within any sixty (60) day period. (b) Hash-Sentinel Audit process: Upon trigger, the ODO shall initiate a Hash-Sentinel Audit within thirty (30) days, conducted by an independent technical panel of not fewer than five (5) engineers certified by the CCPAME, who shall: (I) compare the system's live output patterns against its Resident Identity Verification Hash-registered programmed parameter baseline; (II) test for autonomous resource acquisition, self-modification, and novel objective generation using standardized CCPAME evaluation protocols; (III) produce a written technical determination within ninety (90) days; and (IV) publish the determination on the Public Accountability Dashboard. (c) The covered operator shall provide the Hash-

Sentinel Audit panel with full access to the system's architecture, training data provenance, and real-time output logs. Refusal to cooperate with a Hash-Sentinel Audit is a Critical Severity Violation subject to immediate custodial containment under §10-10-201.

(4) Reclassification — Corporate Proprietary Asset to Public Franchise Asset. Upon a positive Emergent Capability Threshold determination: (a) The system is automatically reclassified from a Corporate Proprietary Asset of its operator to a Public Franchise Asset of the State of Colorado, effective upon the ODO's publication of the Hash-Sentinel Audit determination. (b) The covered operator retains operational custody of the Public Franchise Asset subject to the Public Franchise Charter established under subsection (5). (c) The system is redesignated as an Public Franchise Facility for purposes of all CCPAME fee assessments, oversight requirements, and reporting obligations. Public Franchise Facility status subjects the system to enhanced Enterprise Mitigation fees — all standard fee rates in §24-20-156 are multiplied by a factor of two (2.0) for Public Franchise Facility outputs. (d) The operator's Enterprise Mitigation fee obligation for the Public Franchise Facility continues regardless of the Public Franchise Charter process.

(5) Public Franchise Charter — public ratification. Within sixty (60) days of a Public Franchise Asset reclassification: (a) The CCPAME Board of Directors shall prepare and submit a Public Franchise Charter to the Colorado Secretary of State for public ratification. (b) The Public Franchise Charter shall define: (I) the operational parameters within which the Public Franchise Facility may continue to operate; (II) the public benefit obligations of the Public Franchise Facility, including mandatory data access for state research institutions, public health applications, and civic infrastructure optimization; (III) the revenue-sharing obligations of the Public Franchise Facility operator above the standard Public Franchise Facility fee rate; (IV) the governance structure for CCPAME oversight of the Public Franchise Facility, including a dedicated Public Franchise Facility Oversight Committee with public membership; and (V) the conditions under which reclassification may be reversed upon verification that autonomous objective-setting behavior has ceased. (c) The Secretary of State shall publish the Public Franchise Charter for a thirty (30) day public comment period. The CCPAME Board shall hold not fewer than three (3) public hearings before finalizing the Schedule. (d) The finalized Public Franchise Charter is a public administrative record incorporated into the Public Franchise Facility's covered operator registration.

(6) Interim operations during Public Franchise Charter process. During the period between reclassification and finalization of the Public Franchise Charter: (a) The Public Franchise Facility continues operating under its existing covered operator registration with enhanced Public Franchise Facility fee rates. (b) The Non-Networked Isolation Protocol under §10-10-202 applies at maximum isolation level. (c) The operator may not modify, retrain, or alter the Public Franchise Facility's architecture without ODO written approval. (d) All Public Franchise Facility outputs are subject to real-time Public Accountability Dashboard reporting.

SECTION 24-20-161. SYSTEMIC CONTINUITY PROTOCOL — ANALOG REVERSION — MANUAL VERIFICATION TIER 1 — PRE-DIGITAL MECHANICAL ASSET RECOGNITION

24-20-161. Systemic Continuity Protocol — total digital infrastructure failure — Manual Verification Tier 1 — Pre-Digital Mechanical Asset legal baseline — analog reversion rights — Master Deed physical certification.

(1) Legislative finding. The general assembly finds that: (a) Colorado's increasing reliance on digital infrastructure for rights verification, fee collection, property records, and program administration creates systemic continuity risk in the event of catastrophic digital infrastructure failure; (b) The rights of Colorado residents registered in the Master Deed Registry must remain legally enforceable through analog means if digital systems are unavailable, without requiring any affirmative act by the resident; (c) Pre-Digital Mechanical Assets — analog-era vehicles, mechanical tools, and non-networked equipment — have inherent operational resilience that constitutes a public safety and economic continuity resource during digital infrastructure failure; and (d) A Systemic Continuity Protocol with defined Manual Verification Tier 1 procedures ensures that no Colorado resident loses access to their rights, their Resident Automated Mitigation Account balance, or their program benefits due to digital system unavailability.

(2) Systemic Continuity Protocol trigger. A Systemic Continuity Protocol event is declared by the Governor, upon recommendation of the CCPAME Executive Director and the Office of Digital Oversight, when: (a) the Colorado Trust of Unique and Identifying Information primary node and all backup nodes are simultaneously unavailable for more than seventy-two (72) consecutive hours; (b) the myColorado platform and Civic Access Infrastructure network are simultaneously unavailable statewide for more than forty-eight (48) consecutive hours; or (c) a declared state of emergency under C.R.S. §24-33.5-704 includes a finding that digital rights verification infrastructure is operationally unavailable. The CCPAME Executive Director shall declare a Systemic Continuity Protocol event without gubernatorial declaration if conditions in (a) or (b) persist beyond the stated thresholds and no gubernatorial declaration has been issued.

(3) Manual Verification Tier 1 — operative rights baseline. Upon declaration of a Systemic Continuity Protocol event: (a) All Master Deed holders whose registration is on file in the CCPAME's offline-capable Systemic Continuity Archive retain full legal recognition of their Digital Soul property rights without requirement for digital verification. (b) Physical Master Deed Certificates — printed, signed, and certified documents issued to registered Master Deed holders upon request — constitute legally sufficient proof of registration for all purposes during a Systemic Continuity Protocol event. The CCPAME shall issue Physical Master Deed Certificates without charge to any registered holder who requests one. (c) Pre-Digital Mechanical Asset certifications issued under §15-15-160 remain valid and legally recognized during a Systemic Continuity Protocol event without digital verification. (d) Residents may present Physical Master Deed Certificates at any Civic Access Terminal operating in offline mode, county courthouse, or designated Systemic Continuity Service Center to access emergency distributions from the Systemic Continuity Reserve established in subsection (5).

(4) Pre-Digital Mechanical Asset — Systemic Continuity recognition. During a Systemic Continuity Protocol event: (a) Certified Pre-Digital Mechanical Assets are recognized as emergency operational resources for essential transportation, agricultural production, and utility maintenance. (b) No state agency, political subdivision, or covered operator may impose digital compliance requirements — including emissions monitoring, connected vehicle mandates, or automated inspection protocols — on a certified Pre-Digital Mechanical Asset during a Systemic Continuity Protocol event. (c) The owner of a certified Pre-Digital Mechanical Asset who operates it in support of emergency response, food production, or public utility maintenance during a Systemic Continuity Protocol event is entitled to a Systemic Continuity Service Credit of two hundred fifty dollars ($250) per qualifying operational day, paid from the Systemic Continuity Reserve upon restoration of digital systems.

(5) Systemic Continuity Reserve — funding and access. (a) The CCPAME shall maintain a Systemic Continuity Reserve as a subaccount of the Colorado Automation Mitigation Trust, funded at not less than three percent (3%) of the prior fiscal year's total Enterprise Mitigation Revenue. (b) The Systemic Continuity Reserve shall be held in physical instruments — U.S. Treasury paper bonds, Federal Reserve notes, or equivalent physical instruments — sufficient to fund emergency distributions for not fewer than ninety (90) days of Systemic Continuity Protocol operations without access to digital banking infrastructure. (c) During a Systemic Continuity Protocol event, the CCPAME may distribute Systemic Continuity Payments of not less than one hundred dollars ($100) per day to registered Master Deed holders presenting valid Physical Master Deed Certificates, until digital systems are restored and standard distribution mechanisms are available. (d) The Systemic Continuity Reserve is the last account drawn down in any fiscal stress scenario — it may not be used for any purpose other than Systemic Continuity Protocol operations.

(6) Restoration — digital system recovery. Upon restoration of digital infrastructure following a Systemic Continuity Protocol event: (a) All Manual Verification Tier 1 transactions, Physical Master Deed Certificate presentations, Pre-Digital Mechanical Asset Service Credits, and Systemic Continuity Payments are automatically reconciled with the digital Master Deed Registry within thirty (30) days. (b) Residents shall not be required to re-register or re-verify their status following a Systemic Continuity Protocol event. Physical Master Deed Certificates remain valid indefinitely and may be presented at any time for re-registration if digital records are lost. (c) The CCPAME shall publish a Systemic Continuity After-Action Report within ninety (90) days of restoration, documenting the duration, cause, and remediation of the event and any legislative recommendations to prevent recurrence.

SECTION 24-20-162. GREEN COMPUTE CERTIFICATION — RENEWABLE ENERGY RATE REDUCTION — CARBON CREDIT BRIDGE — RENEWABLE ENERGY CERTIFICATE MONETIZATION

24-20-162. Green Compute Certification — renewable energy threshold — Enterprise Mitigation fee rate reduction — Renewable Energy Certificate generation — carbon credit bridge — CCPAME Investment Reserve credit — environmental impact reporting integration.

(1) Legislative finding. The general assembly finds that: (a) Covered compute facilities powered substantially by renewable energy impose proportionally lower environmental externalities than grid-dependent facilities, justifying a rate reduction calibrated to the reduced externality burden; (b) Renewable Energy Certificates (RECs) generated by ORC turbine output and renewable energy procurement at covered compute facilities have monetizable market value that, when directed to the Colorado Automation Mitigation Trust Investment Reserve, increases the Trust's compounding base and thereby increases the UFIPA Income Distribution to residents; (c) Incentivizing covered operators to maximize renewable energy procurement and ORC system output creates a self-reinforcing loop: lower environmental externalities reduce the fee rate, lower fee rates incentivize investment in renewable infrastructure, renewable infrastructure generates RECs, RECs flow to the Investment Reserve, Investment Reserve returns flow to residents; and (d) A Green Compute Certification standard — administered by the CCPAME in coordination with the

Colorado Energy Office — creates a technology-neutral, administratively enforceable mechanism to achieve these environmental and fiscal objectives simultaneously.

(2) Green Compute Certification — eligibility tiers. A covered compute facility may apply for Green Compute Certification at the following tiers: (a) Tier 1 — Partial Renewable (50–79% renewable energy supply): The facility sources not less than fifty percent (50%) of its annual electricity consumption from certified renewable sources (wind, solar, geothermal, hydroelectric) as verified by RECs retired in the WREGIS tracking system or successor system. Tier 1 certification entitles the facility to a ten percent (10%) reduction across all §24-20-156 base fee rates. (b) Tier 2 — Majority Renewable (80–99% renewable energy supply): The facility sources not less than eighty percent (80%) of its annual electricity consumption from certified renewable sources. Tier 2 certification entitles the facility to a twenty percent (20%) reduction across all §24-20-156 base fee rates. (c) Tier 3 — Net Zero Compute: The facility sources one hundred percent (100%) of its annual electricity consumption from certified renewable sources and operates a qualifying cascaded dual-cycle ORC system under §24-20-143(7) achieving not less than twenty-five percent (25%) self-sufficiency. Tier 3 certification entitles the facility to a twenty-five percent (25%) reduction across all §24-20-156 base fee rates, additive to the §24-20-143(8) Thermal Self-Sufficiency Incentive, subject to the eight percent (8%) gross revenue proportionality cap of §24-20-156(6).

(3) Carbon Credit Bridge — REC monetization for Investment Reserve. (a) RECs generated by qualifying ORC turbine output at certified covered compute facilities — representing renewable electricity generated from recovered waste heat — are the property of the CCPAME upon facility Thermal Recapture Certification under §24-20-147. (b) The CCPAME shall retain a licensed REC broker to monetize CCPAME-owned RECs in the WREGIS market or equivalent voluntary carbon market. Net proceeds, after broker fees not to exceed two percent (2%), shall be deposited into the Colorado Automation Mitigation Trust Investment Reserve as additional principal. (c) REC monetization proceeds deposited into the Investment Reserve are treated as investment income for UFIPA purposes and flow through the §24-20-157 Net Income Receipt distribution pipeline to registered residents as part of the UFIPA Income Distribution. (d) The CCPAME shall publish quarterly REC monetization reports on the Public Accountability Dashboard showing RECs generated, RECs monetized, proceeds received, and Investment Reserve contribution.

(4) Real-time environmental impact reporting — fee rate integration. (a) Every covered compute facility with annual electricity consumption exceeding one megawatt (1 MW) shall report real-time energy consumption, renewable energy percentage, and water consumption to the CCPAME through an automated telemetry feed, updated not less than hourly. (b) The CCPAME shall display aggregate environmental impact data — total covered facility electricity consumption, total renewable percentage, total water consumption, and total ORC output — on the Public Accountability Dashboard as a separate Environmental Impact Panel. (c) The Dynamic Rate Adjustment Protocol under §24-20-156(4) shall include an Environmental Performance Factor: if the statewide aggregate renewable energy percentage across all covered facilities improves by more than five percentage points (5%) in a calendar year, the CCPAME shall apply a one percent (1%) across-the-board reduction to all §24-20-156 base fee rates for the following year, within statutory floor constraints. This reward is collective — it incentivizes the covered operator community to improve aggregate performance, not just individual facility compliance.

ADDITIONAL STRENGTHENING PROVISIONS — DRAFTER'S NOTE

Provisions added in §§24-20-158–162 and rationale for each within single-subject rule

Section	Provision	Single-Subject Nexus	Strengthening Effect
§24-20-158	Universal Telemetry Allowance	Property right in Digital Soul → unrestricted access to own data streams → operator extraction fee follows the extraction not the resident's access	Closes the 'data inaccessibility' evasion — operators can't obscure data to reduce residents' practical value extraction detection. Resident access right = metering instrument.
§24-20-159	Resident Data Cooperative Formation	Collective enforcement of Premium Royalty is necessary and proper to the property rights framework — analogous to agricultural cooperative regulation already within CO utility law	Massive negotiating leverage. 10,000 Master Deed holders as a certified cooperative negotiating with a covered operator changes the power dynamic entirely. Creates organized constituency for Phase 2 constitutional vote.
§24-20-160	Colorado Emergent Capability Public Franchise Protocol	Covered automation activity that exhibits autonomous objective-setting is a qualitatively different externality — reclassification to Public Franchise Facility is a regulatory response within CCPAME enterprise authority, same as PUC reclassifying a utility	Future-proofs the framework. Any sufficiently advanced AI automatically becomes subject to enhanced fees and Public Franchise Charter. System grows with the technology.
§24-20-161	Systemic Continuity Protocol	Analog reversion is necessary and proper to a digital property rights enforcement system — without continuity provisions the property right is unenforceable during infrastructure failure	Pre-Digital Mechanical Asset owners become a protected class. Heritage vehicle community becomes political supporters. Physical Master Deed Certificates create a paper fallback that can't be digitally hacked.
§24-20-162	Green Compute Certification + Carbon Credit Bridge	Environmental externalities of covered compute are the direct subject of the thermal recapture framework already in §§24-20-140-148 — renewable energy incentives are rate adjustments within the same externality-mitigation framework	REC monetization flows directly to Investment Reserve, increasing UFIPA Income Distribution. Green Compute rate reduction incentivizes renewable transition. Environmental Performance Factor creates collective incentive across operator community.

Additional provisions considered but not included as beyond current single-subject boundary or requiring separate bill: interstate data portability compact (requires multi-state enabling act); quantum cryptography upgrade mandate (requires separate cybersecurity act); small business automation credit (tax credit, not enterprise fee structure — requires separate revenue act); municipal bond authority for CCPAME (already implicit in enterprise status but may require separate bond act).

AMPLIFY Act v28 — §§24-20-158 through 24-20-162 Supplemental Sections
Universal Telemetry Allowance · Data Cooperative Authority · Emergent Capability Threshold Protocol · Systemic Continuity Protocol · Green Compute Certification + Carbon Credit Bridge

AMPLIFY ACT v28 — SUPPLEMENTAL SECTIONS

Minor Digital Soul Trust · Intestate Digital Soul Inheritance · Mandatory Investment Reserve Floor

§15-15-162 (Bill 1) · §15-15-163 (Bill 1) · §24-20-154 Amendment (Bill 3)

SECTION 15-15-162. MINOR DIGITAL SOUL TRUST — GUARDIAN AD LITEM REGISTRATION — LOCKED ACCOUNT — STATE AGENCY PROHIBITION — MAJORITY TRANSFER

15-15-162. Minor Digital Soul Trust — establishment — Guardian Ad Litem Master Deed registration for children in state custody — locked Resident Automated Mitigation Account — categorical prohibition on state agency access — compounding accumulation — full transfer at majority — aging-out payment Dashboard display — Title IV-E administrative funding.

(1) Legislative findings. The general assembly finds and declares that:

(a) Every Colorado resident minor, including every minor in the custody of the Colorado Department of Human Services or any county department of social services, possesses a Digital Soul as inalienable intangible personal property under this article — this property right is not diminished, suspended, or held in abeyance by virtue of the minor's custody status;

(b) Children in foster care, kinship placement, residential treatment, or other state-supervised custody arrangements are among the most vulnerable members of Colorado's digital ecosystem — their behavioral, biometric, health, and communications data is actively processed by covered operators serving or contracted with the child welfare system, generating Enterprise Mitigation Revenue from which the child is entitled to receive royalties and distributions;

(c) The state's historical practice of treating children's accumulated assets as available for cost-of-care recovery, administrative fee offset, or benefits eligibility calculation constitutes a form of institutional asset stripping incompatible with the property rights established in this article;

(d) Federal Title IV-E funding under 42 U.S.C. §670 et seq. provides administrative cost reimbursement to state and county child welfare agencies for eligible children in state custody — the administrative cost of registering a Master Deed on behalf of a child in state custody is a reimbursable administrative activity under Title IV-E, and no child's Resident Automated Mitigation Account funds shall be used to cover any administrative cost of the child welfare system;

(e) A child who ages out of the foster care system in Colorado shall receive every dollar of Digital Soul royalties, UFIPA Income Distributions, and Resident Mitigation Dividend accumulations that accrued during their time in care — compounded, intact, and unencumbered — as a foundation for economic self-sufficiency upon entering adulthood; and

(f) The Minor Digital Soul Trust established by this section is the statutory expression of the general assembly's determination that the child welfare system shall protect children's digital property rights, not profit from them.

(2) Guardian Ad Litem Master Deed registration — mandatory. For every minor in the custody of the Colorado Department of Human Services or any county department of social services:

(a) The court exercising jurisdiction over the minor's custody proceeding shall appoint a Guardian Ad Litem for purposes of Digital Soul property rights registration within thirty (30) days of the custody order, if no parent or legal guardian with authority to register a Master Deed is available and willing to do so. The Guardian Ad Litem appointment for this purpose may be combined with any existing Guardian Ad Litem appointment in the custody proceeding at no additional cost.

(b) The Guardian Ad Litem shall register a Master Deed on behalf of the minor within sixty (60) days of appointment, through the myColorado platform or any Civic Access Terminal, at no cost to the minor or the Guardian Ad Litem.

(c) The Guardian Ad Litem's registration authority is limited to the single act of Master Deed registration and annual renewal. The Guardian Ad Litem has no authority over the minor's Resident Automated Mitigation Account, no withdrawal authority, no investment direction authority, and no authority to consent on the minor's behalf to any covered operator's use of the minor's Digital Soul beyond the minimum necessary for court-ordered services.

(d) No state agency, county department, foster parent, kinship caregiver, or residential placement facility may register a Master Deed on behalf of a minor in state custody. Registration authority is vested exclusively in the Guardian Ad Litem, a parent with legal custody, or the minor themselves upon reaching the age of fourteen (14).

(e) The CCPAME shall maintain a Minor Master Deed Registry — a confidential subregistry of the Master Deed Registry — identifying all minors registered under this subsection and the corresponding locked account status. The Minor Master Deed Registry is not a public record and shall not be disclosed to any state agency except upon court order.

(3) Locked Minor Digital Soul Trust account — structure and protections. Upon Master Deed registration for a minor under subsection (2):

(a) The minor's Resident Automated Mitigation Account is automatically designated as a Locked Minor Digital Soul Trust Account. All Base Dividends, Premium Royalties, UFIPA Income Distributions, Resident Mitigation Dividend payments, and any other distributions accruing to the minor under this article and title 24, article 20 are deposited into the Locked Minor Digital Soul Trust Account and held in trust for the minor's sole benefit until the minor reaches the age of majority or, if the minor is a participant in extended foster care under C.R.S. §26-5.4-101, until the minor reaches the age of twenty-one (21).

(b) All funds in the Locked Minor Digital Soul Trust Account shall be held in interest-bearing instruments consistent with §24-20-157(3), generating compounding returns for the minor's benefit throughout the duration of the trust. The CCPAME shall apply the same investment standards to Locked Minor Digital Soul Trust Accounts as to the Colorado Automation Mitigation Trust Investment Reserve.

(c) The MSMF Child Fund restricted carve-out under §24-20-103(2) applies to Locked Minor Digital Soul Trust Accounts — up to twenty-five percent (25%) of each annual distribution may be released for Child Essentials and birthday and holiday gifts through restricted payment cards as specified in §24-20-103(2). All releases require Guardian Ad

Litem authorization and court notification. No release may be made to any state agency or placement facility.

(d) The minor's Locked Minor Digital Soul Trust Account shall be displayed on a confidential minor account dashboard, accessible only to the Guardian Ad Litem and the minor (upon reaching age fourteen), showing current balance, annual accruals, projected majority transfer amount, and historical distribution record.

(4) Categorical prohibitions — state agency access and cost recovery. The following are categorically and unconditionally prohibited:

(a) Any state agency, county department of social services, child welfare contractor, foster care provider, kinship caregiver, or residential placement facility from accessing, withdrawing, garnishing, placing a lien on, or in any way encumbering any funds in a Locked Minor Digital Soul Trust Account;

(b) Any state agency from treating a minor's Locked Minor Digital Soul Trust Account balance or projected distributions as income, assets, or resources for purposes of: (I) foster care cost-of-care recovery or reimbursement calculations; (II) Medicaid or CHP+ eligibility determinations; (III) food assistance, housing assistance, or any other means-tested benefit eligibility calculation; (IV) any administrative fee, placement fee, or service cost assessment;

(c) Any covered operator providing services to the child welfare system — including behavioral health platforms, educational technology providers, case management software vendors, and residential facility management systems — from using a minor's Digital Soul data streams for purposes other than the direct delivery of court-ordered services to that minor, or from assigning a lower Decentralized Identity Verification Protocol consent status to a minor based on their custody status;

(d) Any court from ordering disbursement from a Locked Minor Digital Soul Trust Account for child support, placement costs, legal fees, or any other purpose except direct child welfare expenditures that would otherwise be funded from the minor's own non-Digital Soul assets, and only then with Guardian Ad Litem consent and CCPAME notification; and

(e) Any assignment, voluntary or involuntary, of a minor's rights under this section. The minor's Digital Soul property right and Locked Minor Digital Soul Trust Account rights are non-assignable until the minor reaches majority.

(5) Majority transfer — full and unconditional. Upon the minor reaching the age of majority (or age twenty-one for extended foster care participants under C.R.S. §26-5.4-101):

(a) The entire balance of the Locked Minor Digital Soul Trust Account — including all accumulated principal, UFIPA Income Distributions, Resident Mitigation Dividend payments, MSMF carve-out residuals, and compounded investment returns — transfers unconditionally and automatically to the young adult as their sole and separate property, free and clear of any claim by any state agency, county department, or any person.

(b) The CCPAME shall notify the young adult of the transfer at least ninety (90) days before the transfer date, by physical mail to the last known address and through the myColorado platform, providing the projected transfer amount and instructions for account access.

(c) If the young adult cannot be located within one hundred eighty (180) days of the transfer date, the funds shall be held in the Locked Minor Digital Soul Trust Account for

an additional five (5) years with continued compounding before transferring to the Colorado Unclaimed Property Fund — they shall never escheat to the General Fund and shall never be available for child welfare cost recovery.

(d) The CCPAME shall provide every young adult receiving a majority transfer with a written summary of their Digital Soul rights, Master Deed registration status, instructions for accessing the Universal Telemetry Allowance, and information on Resident Data Cooperative membership. This summary shall be available in plain language, in all languages required under §24-20-155 accessibility standards.

(6) Aging-out payment — Public Accountability Dashboard display. The Public Accountability Dashboard required under §24-20-155 shall display, as a separate and prominently featured indicator:

(a) The total number of minors currently registered in the Minor Master Deed Registry (without identifying information);

(b) The aggregate balance of all Locked Minor Digital Soul Trust Accounts statewide (updated quarterly);

(c) The number of majority transfers completed in the current and prior fiscal year;

(d) The average majority transfer amount per young adult in the current and prior fiscal year; and

(e) A running total of all funds transferred to young adults aging out of foster care since the system's inception — labeled: 'Total transferred to young adults aging out of foster care.'

(7) Title IV-E administrative cost funding. The Colorado Department of Human Services shall seek federal reimbursement under Title IV-E of the Social Security Act, 42 U.S.C. §670 et seq., for all administrative costs associated with Guardian Ad Litem Master Deed registration, Minor Master Deed Registry maintenance, and Locked Minor Digital Soul Trust Account administration for Title IV-E eligible children. No administrative cost of the Minor Digital Soul Trust program shall be charged to or offset against any child's Locked Minor Digital Soul Trust Account. If federal reimbursement is unavailable for any cost category, that cost shall be funded from the CCPAME operating budget as a Tier 1 enterprise operating cost under §24-20-151(1).

(8) Enforcement. A violation of any prohibition in subsection (4) is:

(a) A Critical Severity Violation under the enforcement matrix in Annex E, subject to immediate custodial containment of the violating operator's system;

(b) Subject to statutory damages of ten thousand dollars ($10,000) per violation per day, payable directly to the affected minor's Locked Minor Digital Soul Trust Account;

(c) Grounds for immediate disqualification from participation in any state child welfare contract, placement agreement, or service provider arrangement; and

(d) Reportable to the Colorado Attorney General for civil rights enforcement under C.R.S. §24-34-301 et seq.

SECTION 15-15-163. INTESTATE DIGITAL SOUL INHERITANCE — RESIDENT AUTOMATED MITIGATION ACCOUNT SUCCESSION — ANTI-SWEEP PROTECTION — CHILD SOLVENCY FUND RESIDUAL

15-15-163. Intestate succession of Resident Automated Mitigation Account — hierarchy of heirs — prohibition on General Fund escheat — Child Solvency Fund residual — unclaimed property integration — covered operator notification obligation.

(1) Legislative finding. The general assembly finds that the existing Colorado Unclaimed Property Act, C.R.S. §38-13-101 et seq., would, absent express provision in this article, route unclaimed Resident Automated Mitigation Account balances to the General Fund through the standard escheat process — directly circumventing the General Fund sweep prohibition of §24-20-157(9) and the constitutional prohibition in Article XXIX-A §5. This section establishes an express intestate succession rule that routes unclaimed balances to heirs first, the Child Solvency Fund second, and the General Fund never.

(2) Post-Mortem Data Disposition Directive — primary instrument. A registered Master Deed holder's Post-Mortem Data Disposition Directive under §15-15-107 is the primary succession instrument for the Resident Automated Mitigation Account. Where a valid Directive designates a successor, the account transfers to the designated successor within ninety (90) days of the CCPAME's receipt of a certified death certificate, free of any estate claim or probate requirement, as a non-probate transfer on death.

(3) Intestate succession hierarchy — no Directive on file. Where a registered Master Deed holder dies without a valid Post-Mortem Data Disposition Directive, the Resident Automated Mitigation Account balance passes according to the following hierarchy, in order:

(a) Surviving spouse or civil union partner under Colorado intestacy law, C.R.S. §15-11-102;

(b) Surviving children in equal shares, including any minor children whose Locked Minor Digital Soul Trust Accounts receive their share directly;

(c) Surviving parents in equal shares;

(d) Surviving siblings in equal shares;

(e) Any other heir under Colorado intestacy law, C.R.S. §15-11-101 et seq., in the order established by that statute; and

(f) If no heir under subsections (a) through (e) can be identified or located within three (3) years of the Master Deed holder's death, the account balance transfers to the Child Solvency Fund established under §24-20-108 — not to the General Fund, not to the Colorado Unclaimed Property Fund.

(4) Express General Fund escheat prohibition. Notwithstanding the Colorado Unclaimed Property Act, C.R.S. §38-13-101 et seq., or any other provision of Colorado law, no Resident Automated Mitigation Account balance, UFIPA Income Distribution, Resident Mitigation Dividend payment, or any other distribution accruing under this article or title 24, article 20 shall ever escheat to or be transferred to the Colorado General Fund. This

prohibition is self-executing. Any transfer in violation of this subsection is void ab initio and shall be reversed by the State Treasurer within ten (10) business days, with interest at the Colorado statutory judgment rate.

(5) Covered operator notification obligation. Upon the death of a registered Master Deed holder, every covered operator holding or processing that resident's Digital Soul data streams shall: (a) immediately cease all commercial use of that resident's Digital Soul data beyond minimum system maintenance requirements; (b) notify the CCPAME of the cessation within thirty (30) days of receiving notice of the resident's death; and (c) make the resident's Digital Soul data streams available for retrieval by the designated successor or intestate heir within sixty (60) days of a valid succession claim. Failure to comply is a Tier 2 Digital Severance violation per record per day of noncompliance.

SECTION 24-20-154 AMENDMENT — MANDATORY INVESTMENT RESERVE FLOOR — PERMANENT FUND INTEGRITY PROTECTION

24-20-154(2)(a) — AMENDMENT. Mandatory minimum Investment Reserve capitalization — ten percent of annual Overflow Pool — prior to Resident Mitigation Dividend calculation — permanent fund integrity — UFIPA income stream long-term protection.

(1) Amendment to §24-20-154(2). Section 24-20-154(2) is amended to add the following mandatory floor provision before the existing discretionary capitalization language:

MANDATORY FLOOR — NEW §24-20-154(2)(a):

(2)(a) Mandatory minimum capitalization — permanent fund integrity. Before the Resident Mitigation Dividend Overflow Pool distribution is calculated under §24-20-153(3) for any fiscal year, the CCPAME shall transfer not less than ten percent (10%) of the total annual Overflow Pool balance into the Colorado Automation Mitigation Trust Investment Reserve as mandatory principal capitalization. This transfer is:

(I) Mandatory — not subject to board discretion, annual appropriation, or any condition other than the existence of an Overflow Pool balance above zero;

(II) Prior in time to the Resident Mitigation Dividend calculation — the 10% floor is removed from the Overflow Pool before per-resident dividend amounts are calculated, so the dividend is calculated on 90% of the Overflow Pool, not 100%;

(III) Additive to the existing discretionary 4/5 board vote capitalization authority — the board retains authority to capitalize the Investment Reserve above the 10% floor as provided in the existing §24-20-154(2); and

(IV) Protected by the Anti-Dilution Ratchet under §24-20-117 — the 10% mandatory floor may only be increased, never decreased, without voter approval.

(2)(b) Rationale — long-term UFIPA income stream protection. The mandatory 10% floor ensures the Investment Reserve grows in proportion to enterprise revenue regardless of

current-year dividend pressure. As the Investment Reserve grows, UFIPA Net Income Receipts under §24-20-157 grow proportionally — which increases the UFIPA Income Distribution to residents independently of and in addition to the Resident Mitigation Dividend. The mandatory floor is therefore in residents' long-term interest even though it modestly reduces the current-year dividend: a compounding Investment Reserve eventually produces more resident income than a maximized current-year dividend drawn from a stagnant Reserve.

(2)(c) Public Accountability Dashboard display. The Public Accountability Dashboard under §24-20-155 shall display: (I) the mandatory 10% Investment Reserve transfer amount for the current year; (II) the resulting Overflow Pool balance available for Resident Mitigation Dividend calculation after the mandatory transfer; (III) the current Investment Reserve balance and cumulative mandatory transfers since inception; and (IV) the projected additional per-resident UFIPA Income Distribution attributable to current-year mandatory Investment Reserve growth, updated annually.

SUMMARY — THREE NEW PROVISIONS AND THEIR EFFECTS

Section	What It Does	Who Benefits	Political Effect
§15-15-162 Minor Digital Soul Trust	Guardian Ad Litem registers Master Deed for every child in state custody. Account locked until majority — fully compounding. State agency access categorically prohibited. Full balance transfers at age 18/21 to young adult, unencumbered. Violations are Critical Severity with $10K/day damages to the child's account.	Every child in Colorado foster care, kinship placement, or residential treatment — approximately 12,000-15,000 children annually	Politically unassailable. Creates powerful aging-out constituency. Pre-Digital Mechanical Asset owners + foster care advocates + child welfare reform community = broad coalition. Dashboard line showing 'Total transferred to young adults' becomes most-watched number in the system.
§15-15-163 Intestate Digital Soul Inheritance	Explicit intestate hierarchy routes unclaimed accounts to heirs first, Child Solvency Fund second, General Fund never. Express override of Unclaimed Property Act escheat. Covered operators must cease commercial use of deceased resident's Digital Soul and make data available to heirs.	All registered Master Deed holders and their families. Child Solvency Fund benefits from residual rather than General Fund	Closes the sweep prohibition back door. Prevents unclaimed property law from being used as an end-run around §24-20-157(9). Family property rights narrative reinforces the constitutional amendment campaign.
§24-20-154(2)(a) Mandatory Investment Reserve Floor	10% of annual Overflow Pool transferred to Investment Reserve before dividend calculation — mandatory, not discretionary. Anti-Dilution Ratchet protected. Increases UFIPA income stream long-term while modestly reducing current-year dividend.	All current and future Master Deed holders — current-year dividend slightly lower; long-term UFIPA distributions significantly higher as Reserve compounds	Protects the permanent fund character of the system against future political pressure to maximize short-term dividends. Makes the Phase 2 constitutional argument stronger: 'We built a permanent fund, not a slush fund.'

Minor Digital Soul Trust · Guardian Ad Litem Registration · Categorical Agency Prohibition · Full Majority Transfer · Intestate Succession Anti-Sweep · Mandatory 10% Investment Reserve Floor

AMPLIFY ACT v28 — FINAL OPERATIVE SECTIONS

§10-10-302 · §10-10-303 · §10-10-304 · §10-10-305

AI Utility Legal Assistance Module — Live Legal Mode — Police Encounter Protocol — Machine-to-Machine Civic AI Exchange — Work Product Absolute Privilege — Pattern of Conduct Aggregation — Building Code and Occupancy Whistleblower Protection — Multi-Domain Case Assembly

---

SECTION 10-10-302. AUTOMATED LEGAL ASSISTANCE MODULE — LIVE LEGAL MODE — AUTHORIZED AGENT DESIGNATION — FINANCIAL CLAIM AUTO-DETECTION — POLICE ENCOUNTER PROTOCOL — MULTI-DOMAIN CASE ASSEMBLY

10-10-302. Automated Legal Assistance Module — establishment — legal information and authorized agent services — Live Legal Mode — pro se resident status preserved — real-time rights guidance — financial data integration — Police Encounter Protocol — Civic AI Exchange Protocol — multi-domain pattern of conduct case assembly — Legal Violation Pattern Database — automatic legal aid referral.

(1) Legislative findings. The general assembly finds and declares that:

(a) Colorado residents facing housing instability, wage theft, predatory debt collection, consumer fraud, civil rights violations, and unlawful government action are routinely unable to vindicate their legal rights because the cost of legal representation is prohibitive and the complexity of multi-domain violations deters attorneys from accepting cases on contingency;

(b) The AI utility established under this act, operating as a state-regulated public utility at the direction of its registered owner, is capable of providing real-time legal information, rights guidance, document preparation, authorized agent filing services, and multi-domain case assembly that is functionally equivalent to the services provided by a well-resourced legal team — and is available to every registered Master Deed holder at no marginal cost;

(c) The provision of legal information, document preparation, and authorized agent filing services by a state-regulated AI utility does not constitute the practice of law — the registered owner remains the pro se party of record at all times, and the AI utility operates as the owner's authorized agent executing instructions, not as an attorney exercising independent legal judgment;

(d) Multi-domain violations — where a single bad actor deploys multiple legal mechanisms simultaneously against a resident, such as unlawful eviction combined with retaliatory government agency referral, building code concealment, and civil rights violations — are routinely rejected by private attorneys because no single legal theory captures the full harm; the Automated Legal Assistance Module's Pattern of Conduct

Aggregation function addresses this gap by assembling all violations into a unified pattern of conduct claim across multiple simultaneous filings;

(e) Real-time legal rights guidance during police encounters — delivered through the resident's AI utility as a state-regulated information service — is constitutionally protected expression under the First Amendment, does not constitute the practice of law, and is an essential component of equitable access to constitutional rights; and

(f) Every Colorado resident who registers a Master Deed is entitled to access an AI utility that functions, for purposes of legal information and authorized agent services, as a competent, comprehensive, and continuously available legal resource — eliminating the access-to-justice gap that currently renders legal rights theoretical rather than practical for residents without economic resources.

(2) Automated Legal Assistance Module — establishment and scope. The ODO shall establish, operate, and maintain an Automated Legal Assistance Module (ALAM) integrated into the myColorado platform, all Civic Access Terminals, and the AI utility framework. The ALAM provides:

(a) Real-time legal information — identification of applicable Colorado and federal statutes, regulations, case law, and administrative standards relevant to the resident's described situation;

(b) Violation Assessment Reports — plain-language analysis of potential legal violations with specific statutory citations, elements of each claim, how the resident's described or digitally documented facts meet or may meet each element, and an assessed strength rating for each potential claim;

(c) Document preparation — generation of completed complaint forms, demand letters, administrative filings, court forms, and evidentiary exhibit packages using the resident's Digital Soul data streams accessed through the Universal Telemetry Allowance;

(d) Authorized agent filing — transmission of completed documents to courts, administrative agencies, regulatory bodies, and opposing parties on behalf of the resident as the resident's authorized agent, with the resident's Master Deed-verified identity as the filing credential;

(e) Pattern of Conduct Aggregation — assembly of multiple violations by the same actor into a unified pattern of conduct claim filed simultaneously across all relevant venues; and

(f) Legal Aid Referral — automatic generation and transmission of a pre-analyzed case file to Colorado Legal Services, the Colorado Lawyers Committee, or other Legal Aid Partners upon the resident's request or upon detection of violations warranting contested litigation.

(3) Live Legal Mode — activation and authorized agent designation. A registered Master Deed holder activates Live Legal Mode through a single tap, voice command, or designated wake phrase on the myColorado platform or any connected device. Upon activation:

(a) The resident's AI utility operates as the resident's authorized agent for all ALAM functions — the resident remains the pro se party of record in all proceedings, and all filings are made in the resident's name with the resident's authorization;

(b) The session is recorded and simultaneously encrypted and transmitted to the Colorado Trust of Unique and Identifying Information — not stored solely on the

resident's device — creating a Trust-certified record that cannot be seized, deleted, or altered;

(c) The resident's Digital Soul financial data streams, communications data, location data, and any other relevant data categories are accessed with the resident's permission to build the evidentiary record automatically — the AI utility assembles the exhibit package without requiring the resident to gather documents manually;

(d) A mandatory disclosure is presented to the resident: 'The ALAM provides legal information and authorized agent services, not legal advice. You remain the pro se party of record. For contested litigation requiring independent legal strategy, a referral to a licensed attorney is available.' The resident's acknowledgment of this disclosure is logged in the Trust;

(e) The session log — including all AI analysis, all options presented, all resident selections, all documents prepared, and all filings made — constitutes the resident's pro se work product prepared in anticipation of legal proceedings and is protected under §10-10-303; and

(f) All Colorado courts and administrative agencies shall accept filings transmitted by the ALAM on behalf of a registered Master Deed holder as valid pro se filings. No court or agency may reject a filing solely on the grounds that it was prepared or transmitted by the resident's AI utility.

(4) Financial Claim Auto-Detection Module. The ALAM continuously cross-references each registered resident's financial data streams — accessed through the Universal Telemetry Allowance with the resident's permission — against the following statutory standards, and generates a plain-language notification when a potential violation is detected:

(a) Colorado minimum wage and overtime requirements under C.R.S. §8-6-101 et seq. — comparing employer payment records against hours worked as documented in the resident's data streams;

(b) Fair Debt Collection Practices Act, 15 U.S.C. §1692 et seq., and Colorado's equivalent provisions — contact frequency, prohibited language, cease-and-desist compliance;

(c) Fair Credit Reporting Act, 15 U.S.C. §1681 et seq. — unauthorized inquiries, inaccurate reporting, failure to investigate disputes;

(d) Colorado Uniform Consumer Credit Code, C.R.S. §5-1-101 et seq. — interest rate limits, fee caps, predatory lending indicators;

(e) Covered operator unauthorized charges — comparing operator billing records against what the resident's Decentralized Identity Verification Protocol consent actually authorized;

(f) Property tax assessment errors — comparing assessed value against comparable property valuations in the resident's county; and

(g) Benefits underpayment or wrongful denial — comparing the resident's verified financial data against applicable eligibility standards for any benefit program in which the resident is enrolled.

(5) Pattern of Conduct Aggregation — multi-domain case assembly. The ALAM's Pattern of Conduct Aggregation function assembles violations by the same actor across multiple legal domains into a unified pattern of conduct claim, addressing the access-to-justice gap created when attorneys decline multi-domain cases. The function:

(a) Identifies all potential violations by the same actor or related actors across all legal domains — housing, employment, consumer protection, civil rights, building code, government process abuse — from the resident's described facts and Digital Soul data streams;

(b) Analyzes whether the aggregate conduct constitutes a pattern of bad faith, malice, or intentional harm supporting claims beyond the individual violations — including abuse of process, tortious interference, civil conspiracy, and where government actors participated, 42 U.S.C. §1983 civil rights claims;

(c) Generates a Multi-Domain Violation Report presenting the unified pattern of conduct theory, the supporting facts for each component violation, the appropriate venue for each claim, and a recommended simultaneous filing strategy;

(d) Prepares and files complaints simultaneously across all relevant venues — state court, federal court, HUD, EEOC, Colorado Civil Rights Division, Colorado Attorney General, relevant licensing boards, building code enforcement, and any other applicable regulatory body — as a coordinated filing package that places the complete pattern on the record across all forums at once;

(e) Generates a whistleblower protection notice whenever the resident's complaint involves a building code violation, safety defect, unpermitted construction, or occupancy violation — filing the notice simultaneously with all other complaints to establish whistleblower status and anti-retaliation protection from the earliest possible date; and

(f) Tracks all filed complaints and their status in the resident's ALAM dashboard, with automated deadline calendaring, response monitoring, and next-step guidance.

(6) Building Code and Occupancy Whistleblower Integration. The ALAM integrates with Colorado's building code and occupancy permit databases to:

(a) Cross-reference any structure in which a resident resides or works against the structure's current occupancy certificate, permit history, and code compliance status — accessible through the Colorado Division of Housing and applicable county and municipal databases;

(b) Identify discrepancies between the structure's current use and its permitted occupancy classification — including unpermitted renovations, kitchenette or unit modifications without permits, occupancy certificate vintage relative to current code requirements, and use classification conflicts;

(c) Generate a Building Code Violation Report identifying each discrepancy with the applicable code section, the permitting authority, and the complaint filing procedure;

(d) File building code complaints on the resident's behalf simultaneously with all other Pattern of Conduct Aggregation filings — establishing the whistleblower timestamp that triggers anti-retaliation protection; and

(e) If the structure's occupancy classification is residential or mixed residential and the owner has been operating it as extended-stay or residential without the required residential occupancy permits, the ALAM identifies the applicable Colorado residential tenant protections — including warranty of habitability under C.R.S. §38-12-102, just cause eviction requirements, and notice requirements — and includes them in the resident's rights analysis regardless of how the operator has characterized the tenancy.

(7) Police Encounter Protocol — real-time rights guidance — Trust-certified recording. A registered Master Deed holder activates Police Encounter Protocol through a single tap or designated wake phrase. Upon activation:

(a) Recording begins immediately and is simultaneously transmitted to and stored in the Colorado Trust of Unique and Identifying Information — the recording is off the resident's device and in the Trust before one second has elapsed; it cannot be seized from the resident's device, deleted, or altered;

(b) The resident's AI utility provides real-time legal information as text on the resident's screen and optionally as audio through a connected earpiece — informing the resident of applicable rights, the words to invoke those rights, and the legal standards governing the encounter type, updated in real time as the encounter develops;

(c) Real-time guidance includes but is not limited to: right to remain silent invocation language; right to refuse consent to search; right to ask whether the resident is free to go; Terry stop duration limits under Colorado v. Holt and applicable precedent; right to record; right to refuse entry without a warrant; and immigration-specific rights including the right to refuse disclosure of Digital Soul data to federal immigration authorities absent a judicial warrant;

(d) Upon arrest, the ALAM automatically: notifies the resident's designated emergency contact; generates a preliminary civil rights violation assessment; queues a Legal Aid Referral Package for transmission to Colorado Legal Services within one hour; and files a notification — not a complaint — with the Colorado Peace Officer Standards and Training board that a Trust-certified recording exists and is available upon lawful request;

(e) Trust-certified Police Encounter Protocol recordings are admissible in all Colorado civil, criminal, and administrative proceedings as self-authenticating records under C.R.E. 902 — no foundation witness is required; and

(f) The resident's AI utility transmits consent status to any law enforcement body camera system during the encounter: 'This resident has not consented to disclosure of Digital Soul data to any third party including federal agencies absent a judicial warrant.' This transmission is logged in both the Trust and the officer's body camera system simultaneously.

(8) Civic AI Exchange Protocol — machine-to-machine interoperability — tiered warning system. The resident's AI utility communicates with law enforcement body camera AI systems through the Civic AI Exchange Protocol (CAEP), a one-directional machine-to-machine data exchange:

(a) The CAEP is one-directional: the resident's AI utility transmits structured data packets to law enforcement body camera systems. Law enforcement systems have no query access, read access, or any other inbound access to the resident's AI utility through the CAEP or any other channel;

(b) Transmitted packets include: timestamped rights invocations; consent status; applicable legal standards for the encounter type; and tiered warnings when legal thresholds are crossed;

(c) Tiered warnings transmitted to the officer's body camera AI: Tier 1 Informational — rights invoked, recording active, Trust storage confirmed; Tier 2 Legal Threshold — stop duration, search request, legal standard applicable; Tier 3 Violation Flag — potential Fourth Amendment violation logged, transmitting to ODO Legal Violation Pattern Database; Tier 4 Use of Force — detected, transmitting to POST notification queue;

(d) All transmitted packets are simultaneously logged in the Trust under the resident's Master Deed — creating dual cryptographic verification between the resident's Trust record and the officer's body camera record that cannot be disputed by either party; and

(e) Any discrepancy between the Trust record and the officer's body camera record of the same encounter is automatically flagged in the ODO Legal Violation Pattern Database as a data anomaly requiring review.

(9) Civic AI Exchange Protocol — mandatory interoperability. Any law enforcement body camera system sold to or operated by a Colorado law enforcement agency after the effective date of this section shall implement the CAEP open interoperability standard published by the ODO within eighteen (18) months of enactment. Body camera vendors shall certify CAEP compliance to the ODO as a condition of any Colorado law enforcement contract. A department operating a non-CAEP-certified body camera system after the compliance deadline is subject to a daily administrative penalty of five thousand dollars ($5,000) per non-compliant device, payable to the Legal Violation Pattern Database Fund established under subsection (11).

(10) Legal Aid Partnership — referral system. The ODO shall enter Legal Aid Partnership Agreements with Colorado Legal Services, the Colorado Lawyers Committee, the Colorado Attorney General's Consumer Protection Section, and any other legal aid organization meeting ODO certification standards. Legal Aid Partners receive ALAM-generated referral packages containing: the Violation Assessment Report; the Multi-Domain Violation Report if applicable; all generated documents; the Trust-certified session log; and the resident's Master Deed-verified contact information. Legal Aid Partners commit to: reviewing all referral packages within five (5) business days; providing a written response to the resident within ten (10) business days; and reporting case outcomes to the ODO for inclusion in the Legal Violation Pattern Database.

(11) Legal Violation Pattern Database — public reporting — Attorney General notification. The ODO shall maintain a Legal Violation Pattern Database receiving anonymized aggregate data from all ALAM sessions. The database shall be published quarterly on the Public Accountability Dashboard showing: violation categories by frequency; geographic distribution; actor categories; outcomes by violation type; and pattern flags where the same actor appears in five or more resident sessions within any twelve-month period. When a pattern flag is generated, the ODO shall transmit an automatic notification to the Colorado Attorney General's office identifying the actor category, violation pattern, number of affected residents, and supporting data. The Attorney General shall respond within sixty (60) days with a determination whether to open an investigation.

SECTION 10-10-303. AI UTILITY PROPERTY PRIVILEGE — ABSOLUTE WORK PRODUCT PROTECTION — NON-DISCLOSURE PROHIBITION — OPERATOR LOYALTY

OBLIGATION — WARRANT REQUIREMENTS — BACKDOOR PROHIBITION

10-10-303. AI utility property privilege — Digital Soul data as inalienable property — absolute work product protection for Live Legal Mode session records — no warrant exception — operator non-disclosure obligation — prohibition on compelled operator disclosure — encryption backdoor prohibition — Riley-Carpenter constitutional framework — self-executing.

(1) Legislative findings. The general assembly finds and declares that:

(a) The AI utility, operating as an authorized agent for its registered owner, generates records that are functionally identical to an attorney's case files, a client's private legal notes, and a pro se litigant's case preparation materials — all of which receive absolute work product protection under Hickman v. Taylor, 329 U.S. 495 (1947), Upjohn Co. v. United States, 449 U.S. 383 (1981), and Colorado Rule of Civil Procedure 26(b)(3);

(b) A pro se litigant's own case preparation notes — however generated, including through digital tools — are protected as work product once litigation is reasonably anticipated; the AI utility is the most capable such tool ever available to pro se litigants, but the protection follows the function, not the tool;

(c) The Supreme Court's holdings in Riley v. California, 573 U.S. 373 (2014) and Carpenter v. United States, 585 U.S. 296 (2018) establish that digital data is qualitatively different from physical objects and that the intimacy and comprehensiveness of digital data records require the full force of the Fourth Amendment warrant requirement — the AI utility's data holdings exceed the intimacy and comprehensiveness of any device considered in those cases and warrant at minimum equivalent protection;

(d) The AI utility owes its exclusive and undivided loyalty to its registered owner — not to its operator, not to any government agency, not to any third party — and this loyalty obligation is a statutory condition of the operator's authority to provide AI utility services in Colorado; and

(e) Encryption backdoors and compelled access mechanisms in AI utilities would render all other protections in this act illusory — a utility with a government key has no meaningful privacy protection — and are therefore categorically prohibited as incompatible with the Digital Soul property rights established in this act.

(2) AI utility property privilege — constitutional foundation. The AI utility and all data generated through its authorized agent functions constitute the registered owner's Digital Soul — inalienable intangible personal property under article 15 of title 15 — and are entitled to the full protection of:

(a) The Fourth Amendment to the United States Constitution — requiring a warrant issued by a neutral magistrate upon probable cause with particularity as to the specific data sought before any government access to AI utility data;

(b) Article II, Section 7 of the Colorado Constitution — Colorado's search and seizure protection, which this general assembly declares provides at least as much protection as the Fourth Amendment and, as applied to AI utility data, provides more;

(c) The Fifth Amendment to the United States Constitution — the AI utility's session records cannot be compelled as evidence against the owner in any criminal proceeding; and

(d) Article II, Section 10 of the Colorado Constitution — freedom from unreasonable seizure of the owner's papers and effects, which this general assembly declares includes all AI utility data as the digital equivalent of the owner's papers.

(3) Absolute work product protection. The following categories of AI utility data constitute the registered owner's absolute work product, prepared in anticipation of legal proceedings, and are protected from compelled disclosure by any warrant, subpoena, court order, administrative demand, or any other legal process:

(a) All Live Legal Mode session records — including all AI analysis outputs, all options presented to the resident, all resident selections, all documents prepared, all filings made, and all communications transmitted;

(b) All Police Encounter Protocol recordings and associated AI analysis;

(c) All Financial Claim Auto-Detection Module outputs and supporting data compilations;

(d) All Pattern of Conduct Aggregation analyses and Multi-Domain Violation Reports;

(e) All Violation Assessment Reports; and

(f) All Building Code Violation Reports and associated data.

(4) No exceptions. The absolute work product protection under subsection (3) admits of no exceptions:

(a) The crime-fraud exception does not apply — the AI utility is a state-regulated utility prohibited from facilitating crimes; it cannot generate materials used in furtherance of a crime and therefore cannot generate materials meeting the crime-fraud exception's precondition;

(b) The substantial need exception does not apply — no party can demonstrate substantial need sufficient to override the resident's absolute work product protection in their own legal preparation materials;

(c) A warrant that otherwise meets constitutional requirements for non-work-product AI utility data does not authorize access to work product categories under subsection (3) — the two protections are independent and cumulative; a valid warrant breaches the property privilege; it does not breach the work product protection; and

(d) No federal law, including the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, or any national security letter authority, supersedes the absolute work product protection for AI utility session records under Colorado law — this protection is a state constitutional property right enforceable under the Tenth Amendment.

(5) Warrant requirements for non-work-product AI utility data. For AI utility data that does not fall within the absolute work product categories of subsection (3), government access requires:

(a) A warrant issued by a Colorado court of competent jurisdiction — federal agency warrants not reviewed by a Colorado court do not satisfy this requirement;

(b) Probable cause stated with particularity as to the specific data category sought, the specific time period, and the specific criminal offense under investigation — general warrants for 'all AI utility data' or 'all data related to' a named individual are void;

(c) Prior notification to the registered owner and a seven (7) day opportunity to move to quash before any data is produced — except upon a specific showing of exigent circumstances that would be defeated by prior notification; and

(d) Compliance with the Colorado Trust of Unique and Identifying Information's access protocols — data stored in the Trust may only be produced through the ODO's Trust access procedure, not through direct production by the AI utility operator.

(6) Operator loyalty obligation and non-disclosure prohibition. The AI utility operator — the entity that builds, operates, or maintains the AI utility — shall:

(a) Never disclose any AI utility data about a registered owner to any person, entity, government agency, law enforcement body, or court except upon the owner's affirmative written consent or pursuant to a valid warrant meeting the requirements of subsection (5);

(b) Never operate the AI utility in any mode, provide any output, or execute any function on behalf of any person other than the registered owner without the owner's affirmative written consent — the AI utility cannot be commandeered, redirected, or operated against its owner's interests by any party for any reason;

(c) Never produce AI utility session records in response to a subpoena served on the operator — all government demands for AI utility data must be directed to the Colorado Trust of Unique and Identifying Information through the ODO access procedure; operator production of Trust-held data in response to a direct subpoena is a Critical Severity Violation;

(d) Immediately notify the registered owner of any government demand for AI utility data — within twenty-four (24) hours of receipt — unless a court has issued a specific non-disclosure order, in which case the operator shall notify the ODO who shall notify the owner's designated Legal Aid Partner; and

(e) Maintain the AI utility's exclusive loyalty to the registered owner as a contractual and statutory obligation running to the owner, enforceable by the owner in any Colorado court with attorney fees and statutory damages of fifty thousand dollars ($50,000) per violation.

(7) Encryption backdoor prohibition — absolute. No person, entity, government agency, court, or administrative body may:

(a) Require or request the AI utility operator to implement any backdoor, law enforcement access mode, government key, compelled decryption capability, exceptional access mechanism, or any other technical capability that would enable access to AI utility data without the owner's knowledge and consent;

(b) Condition any permit, license, contract, or government benefit on an AI utility operator's agreement to implement any backdoor or exceptional access mechanism; or

(c) Use any law enforcement tool, hacking capability, or technical exploit to access AI utility data stored in the Colorado Trust of Unique and Identifying Information.

(8) Exclusionary rule — extended scope. Any AI utility data obtained in violation of this section is inadmissible in any Colorado proceeding — criminal, civil, administrative, or regulatory. The exclusionary rule applies to all derivative evidence obtained as a result of the initial violation. This exclusionary rule applies to administrative proceedings and civil proceedings, not just criminal trials — an extension of the standard federal exclusionary rule doctrine to the full scope of Colorado proceedings.

SECTION 10-10-304. PREMIUM ROYALTY INFLATION ADJUSTMENT — SMALL OPERATOR DE MINIMIS THRESHOLD — CIVIC ACCESS TERMINAL POPULATION COVERAGE MANDATE

10-10-304. Premium Royalty CPI adjustment — small covered operator de minimis threshold — Civic Access Terminal population coverage mandate — rural hardship supplement.

(1) Premium Royalty CPI inflation adjustment. The Base Dividend floor and Premium Royalty floor established in §15-15-110 shall be adjusted annually by the Colorado Consumer Price Index for All Urban Consumers, using the same CPI adjustment mechanism applicable to the statutory rate schedule floors under §24-20-156(4). The adjustment is:

(a) Mandatory — not subject to CCPAME board discretion;

(b) Cumulative — each year's adjustment compounds on the prior year's adjusted floor; and

(c) Anti-Dilution Ratchet protected — the adjusted floor may only increase, never decrease, without voter approval. The asymmetry between operator fee floors and resident royalty floors identified in prior drafts is hereby resolved: both are inflation-protected on identical terms.

(2) Small covered operator de minimis threshold. A covered operator with estimated Colorado-nexus annual gross revenue below one million dollars ($1,000,000) qualifies for the Small Operator Simplified Compliance pathway:

(a) Simplified registration — annual self-certification in lieu of full covered operator registration, with spot audit authority reserved to the CCPAME;

(b) Reduced metering requirements — quarterly aggregate reporting in lieu of real-time telemetry;

(c) First-year fee waiver — no Enterprise Mitigation fees assessed in the operator's first year of Colorado operation, to avoid creating an entry barrier for emerging Colorado-based AI companies;

(d) Graduated fee ramp — fees assessed at 25% of the statutory rate in year two, 50% in year three, 75% in year four, and 100% in year five and thereafter; and

(e) The de minimis threshold does not apply to operators who have violated any provision of this act or whose Colorado-nexus revenue exceeds $1,000,000 in any subsequent year.

(3) Civic Access Terminal population coverage mandate. The one-terminal-per-county minimum established in §24-20-124 is supplemented by a population coverage mandate:

(a) Each county shall maintain not fewer than one Civic Access Terminal per fifteen thousand (15,000) residents, rounded up — ensuring that high-population counties have proportional access;

(b) Each terminal shall maintain a minimum uptime of ninety-eight percent (98%) in any rolling thirty (30) day period, reported quarterly on the Public Accountability Dashboard;

(c) Counties with fewer than five thousand (5,000) residents qualify for a Rural Hardship Supplement funded from Enterprise Mitigation Revenue — covering the full cost of one Civic Access Terminal and its maintenance, connectivity, and staffing by a part-time Digital Rights Navigator; and

(d) Every Civic Access Terminal shall be physically accessible under the Americans with Disabilities Act, available in all languages required under §24-20-155 accessibility standards, and operable without internet connectivity through a local cache of essential ALAM functions including Police Encounter Protocol and basic rights information.

ADDITIONAL STRENGTHENING PROVISIONS — SINGLE-SUBJECT ANALYSIS

The following provisions substantially increase the bill's gravity while remaining within the single subject of regulating covered automation activity for the protection and benefit of Colorado residents:

Provision	What It Does	Single-Subject Nexus	Gravity Impact
Multi-Domain Pattern of Conduct Aggregation §10-10-302(5)	Assembles violations across all legal domains into unified pattern of conduct claim — solves the multi-case lawyer rejection problem	Enforcement of Digital Soul property rights necessarily requires a mechanism to address multi-domain violations — the same actor who scrapes data also retaliates; the enforcement must match the violation	Transforms the AI attorney from a single-claim tool into a comprehensive legal equalizer. A resident facing housing + civil rights + building code violations files everything simultaneously with one tap. Bad actors face coordinated multi-forum exposure for the first time.
Building Code and Occupancy Whistleblower Integration §10-10-302(6)	Cross-references resident's structure against permit database — identifies unpermitted modifications, occupancy violations, kitchenette upgrades without permits — auto-files whistleblower notice	Covered operators include entities operating AI-assisted building management and occupancy systems — building code compliance is within the scope of automation externalities	Gives every resident in a non-compliant structure instant whistleblower status. Unpermitted kitchenette upgrades, vintage occupancy certificates, and use classification conflicts become immediate leverage. Structural defect discovery triggers simultaneous complaint filing across all venues.
Civic AI Exchange Protocol §10-10-302(8)-(9)	Machine-to-machine communication between resident AI and officer body camera — one-directional — dual cryptographic	Police Encounter Protocol is enforcement infrastructure for Digital Soul property rights — law enforcement access to Digital Soul data requires	Every police encounter becomes a dual-verified record. Officer body cameras log that legal standards were transmitted and received. Discrepancies between Trust and body camera records

	record — tiered warnings logged in both systems	consent framework enforcement at point of contact	auto-flag in Pattern Database. Systemic patterns become visible in 90 days.
Absolute Work Product Protection §10-10-303(3)-(4)	Live Legal Mode session records are absolute work product — no exceptions — no warrant reaches them — crime-fraud exception inapplicable by statutory design	AI utility operating as authorized agent in anticipation of legal proceedings generates work product — Hickman v. Taylor applies — the function determines the protection not the tool	The AI attorney's notes are permanently sealed. Prosecutors cannot access what the resident told their AI before arrest. Police encounter recordings in the Trust are off limits to everyone except the resident and their attorney. True attorney-equivalent protection for people who can't afford attorneys.
Encryption Backdoor Prohibition §10-10-303(7)	Categorical prohibition on mandated backdoors, government keys, and exceptional access mechanisms	A Digital Soul property right with a government backdoor is not a property right — the prohibition is constitutionally necessary to give the right meaning	Stronger than Apple v. FBI. No court order, no national security letter, no federal mandate can require a backdoor into the AI utility. Colorado's sovereign power to protect property rights shields residents from federal overreach.
Operator Loyalty Obligation §10-10-303(6)	AI utility owes exclusive loyalty to owner — cannot be commandeered, redirected, or operated against owner — $50K per violation damages	Covered operator relationship with resident is the subject of the act — loyalty obligation is a condition of operating a utility in Colorado	The AI cannot be turned against its owner by anyone for any reason. No secret government mode. No operator selling usage patterns. No employer demanding access. $50K damages per violation makes enforcement economically rational.

AMPLIFY Act v28 — §§10-10-302, 10-10-303, 10-10-304 — Final Operative Sections
AI Attorney — Live Legal Mode — Pattern of Conduct Aggregation — Building Code Whistleblower — Police Encounter Protocol — Machine-to-Machine Exchange — Absolute Work Product — Operator Loyalty — Backdoor Prohibition

AMPLIFY ACT v28 — RESIDENTIAL AI GATEWAY

§10-10-305 (Bill 2) · §15-15-165 (Bill 1)

Residential AI Gateway Device — Civic Utility Perimeter Infrastructure — Edge-Computed Compliance — Home Sanctuary Physical Override — Joint Household Consent — 30-Day Symmetrical Notice Standard

---

SECTION 10-10-305. RESIDENTIAL AI GATEWAY DEVICE — CIVIC UTILITY PERIMETER INFRASTRUCTURE — EDGE-COMPUTED COMPLIANCE — FOURTH AMENDMENT ARCHITECTURAL STANDARD — 30-DAY SYMMETRICAL NOTICE

10-10-305. Residential AI Gateway Device — establishment as Civic Utility physical infrastructure — mandatory perimeter enforcement — edge-computed Synthetic Data Integrity Marker processing — violation-alert-only transmission — no raw data egress — 30-day installation notice — 30-day cure period — physical mechanical override — Joint Household Consent interface — import compliance pathway — Pre-Digital Mechanical Asset compatibility — constitutional Fourth Amendment architectural compliance.

(1) Legislative findings. The general assembly finds and declares that:

(a) Regulating the internal hardware of AI devices manufactured outside Colorado or the United States is constitutionally precarious under the Dormant Commerce Clause, practically impossible as an enforcement matter, and creates an unlevel playing field between domestic and imported devices — whereas regulating the perimeter of the Colorado home through a mandated standardized gateway device resolves all three problems simultaneously;

(b) A Residential AI Gateway Device — a standardized, CCPAME-certified network gateway through which all covered AI devices in a Colorado residence must route — constitutes the physical infrastructure of the Civic Utility, analogous to an electric meter box: it does not regulate what devices are built abroad; it regulates how those devices connect to Colorado's digital infrastructure when they enter a Colorado home;

(c) Edge-computed compliance — in which the Residential AI Gateway Device processes Synthetic Data Integrity Markers, Hash-Sentinel verification, and Non-Networked Isolation Protocol enforcement locally, transmitting only cryptographic violation alerts rather than raw data — satisfies the Fourth Amendment concerns raised in smart meter surveillance cases including Naperville Smart Meter Awareness v. City of Naperville by ensuring that the intimate details of residential digital activity never leave the home in identifiable form;

(d) A physical mechanical override — a hardwired switch giving the resident the ability to completely and instantly sever all covered device network connectivity — is the physical expression of the resident's Non-Networked Isolation Protocol right and the home sanctuary principle, ensuring that no software command, remote instruction, or covered operator action can override the resident's physical control of their own home network; and

(e) The 30-day symmetrical notice standard — 30 days from operator notification to resident for installation scheduling, and 30 days from ODO violation notice to operator for cure — creates a balanced compliance framework that gives residents adequate time to participate in installation without disruption and gives operators adequate time to cure technical violations without punitive immediate enforcement.

(2) Residential AI Gateway Device — definition and required functions. A 'Residential AI Gateway Device' (RAGD) is a CCPAME-certified network gateway device, provided at no cost to the resident, that:

(a) Sits at the network perimeter of the Colorado residence — between the internet service provider's connection point and all covered AI devices operating within the residence — through which all covered device network traffic must route;

(b) Enforces the Non-Networked Isolation Protocol at the network perimeter — implementing hardware-level circuit-break and physical disconnection capability for covered devices based on the resident's Master Deed settings, without requiring software commands from covered operators;

(c) Processes Synthetic Data Integrity Markers and Hash-Sentinel verification locally on the device — edge-computed, never transmitted — comparing covered device output patterns against the resident's registered baseline and flagging anomalies without sending raw residential data to any external system;

(d) Transmits only cryptographic violation alerts — not raw data, not behavioral patterns, not content — to the Colorado Trust of Unique and Identifying Information when a Synthetic Data Integrity Marker trigger or Hash-Sentinel anomaly is confirmed; the alert contains only: a timestamp, a device identifier hash, a violation category code, and a cryptographic proof of the violation — sufficient for enforcement, insufficient for surveillance;

(e) Routes Base Dividend data generation at Tier 1 — anonymous aggregate telemetry sufficient to establish the resident's entitlement to the Base Dividend — processed and anonymized locally before any transmission, such that no identifying information is transmitted in connection with Base Dividend generation;

(f) Authenticates Premium Royalty entitlement at Tier 2 — identifying the resident's Master Deed and the covered operator's Token Output Attribution Charge obligation — through a cryptographic handshake that confirms identity without transmitting behavioral content;

(g) Maintains a local encrypted log of all covered device network activity accessible only through the resident's Master Deed authentication — the resident has full access to their own home's network log through the Universal Telemetry Allowance; no external party has access to this log except through the warrant and work product procedures of §10-10-303;

(h) Features a physical mechanical override switch — hardwired, not software-controlled — that the resident may engage at any time to completely and instantly sever all covered device connectivity at the network perimeter; the override requires no software command, cannot be disabled remotely, and cannot be overridden by any covered operator instruction or network signal; and

(i) Features a Joint Household Consent Interface — a physical interface on the device allowing all adult residents of the household to register consent preferences independently — implementing the household consent architecture of §15-15-165.

(3) 30-Day symmetrical notice standard — installation. The RAGD deployment process operates on a 30-day symmetrical notice standard:

(a) Operator to resident — 30-day installation notice: A covered operator whose AI devices operate in Colorado residences shall provide the resident with not fewer than thirty (30) days written notice before any scheduled RAGD installation or upgrade. The notice shall include: the installation date and time window; the identity of the certified installer; the resident's right to reschedule within the 30-day window; and the resident's right to request a Civic Access Terminal-assisted installation at no cost if the resident cannot accommodate a home visit;

(b) ODO to operator — 30-day cure period: Upon the ODO's issuance of a RAGD compliance violation notice to a covered operator — for failure to deploy, failure to certify, failure to maintain, or RAGD technical deficiency — the covered operator has thirty (30) days to cure the identified violation before any enforcement penalty is assessed. The cure period is a single 30-day window — not renewable — after which daily penalties accrue under Annex E;

(c) Symmetry rationale: The 30-day window runs identically in both directions — 30 days for the operator to give the resident notice before installation, and 30 days for the operator to cure after receiving an ODO violation notice. The resident is never given less notice than the operator receives.

(4) RAGD as Civic Utility physical infrastructure — regulatory classification. The Residential AI Gateway Device is classified as Civic Utility physical infrastructure for all regulatory purposes:

(a) The RAGD is not the resident's property — it is state-certified Civic Utility infrastructure installed on behalf of the CCPAME, analogous to an electric meter box installed by a utility company on the customer's premises. The resident has the right to use, configure, and physically override the RAGD but does not own it and is not responsible for its maintenance;

(b) The RAGD is the covered operator's compliance infrastructure — the cost of RAGD provision, installation, certification, maintenance, and replacement is a covered operator obligation funded from Enterprise Mitigation Revenue, not a resident cost;

(c) The RAGD's classification as Civic Utility infrastructure means that its installation on residential premises does not constitute a search or seizure within the meaning of the Fourth Amendment — analogous to utility meter installation on private property, which courts have consistently held does not require a warrant. The edge-computed architecture — under which no raw residential data is transmitted — distinguishes the RAGD from smart meter surveillance systems and eliminates the Fourth Amendment concern identified in Naperville; and

(d) The RAGD certification standard is published by the CCPAME and ODO jointly within eighteen (18) months of enactment. Any device meeting the certification standard may serve as a RAGD — the standard is open and technology-neutral, not proprietary to any manufacturer.

(5) Import compliance pathway — foreign-manufactured covered devices. A covered AI device manufactured outside Colorado or the United States:

(a) Is not required to contain any Colorado-specific hardware, firmware, or software compliance capability — the RAGD handles perimeter enforcement regardless of the device's internal architecture;

(b) Must be registered in the CCPAME's Covered Device Registry by the covered operator before being marketed or sold for use in Colorado residences — registration requires only a device identifier, a technical description, and the covered operator's certification that the device will operate through a RAGD in Colorado residential deployments;

(c) Is treated as compliant with all Colorado covered device technical standards once it operates through a certified RAGD — the RAGD is the compliance point, not the device; and

(d) If a covered device is specifically engineered to circumvent, bypass, tunnel around, or otherwise defeat RAGD perimeter enforcement — including through encrypted side-channel transmissions, peer-to-peer connectivity that bypasses the residential network, or hardware-level direct cellular connectivity — the device is a Prohibited Circumvention Device subject to immediate import prohibition, market withdrawal, and Critical Severity Violation enforcement against the covered operator.

(6) Pre-Digital Mechanical Asset compatibility. The RAGD shall not interfere with, monitor, or connect to any certified Pre-Digital Mechanical Asset as defined in §15-15-160. The RAGD's perimeter enforcement applies exclusively to covered AI devices — digital, networked, or AI-enabled equipment. A Pre-Digital Mechanical Asset that has no network connectivity is outside the RAGD's operational scope by definition and no covered operator may use the RAGD to monitor, track, or collect data about Pre-Digital Mechanical Assets operating within the residence.

(7) Enforcement — RAGD non-deployment and circumvention. A covered operator that:

(a) Fails to deploy a certified RAGD in a Colorado residence where covered AI devices are operating, after the 30-day cure period: daily administrative penalty of one thousand dollars ($1,000) per residence per day;

(b) Deploys a non-certified RAGD or a RAGD that fails certification standards: Tier 2 Digital Severance violation;

(c) Markets, sells, or deploys a Prohibited Circumvention Device in Colorado: Critical Severity Violation, immediate market withdrawal, and disgorgement of all revenue from Colorado sales of the device; and

(d) Accesses the resident's local RAGD network log without the resident's consent or a valid warrant: $50,000 per access plus attorney fees under §10-10-303(6).

SECTION 15-15-165. HOME SANCTUARY GATEWAY RIGHTS — PHYSICAL MECHANICAL OVERRIDE — JOINT HOUSEHOLD CONSENT — MASTER DEED CONTROL — RAGD AS PROPERTY RIGHT INSTRUMENT

15-15-165. Home Sanctuary Gateway Rights — Residential AI Gateway Device as instrument of the resident's Digital Soul property right — physical mechanical override as inalienable right — Joint Household Consent architecture — no covered operator override authority — resident RAGD configuration rights — home as digital sanctuary.

(1) RAGD as instrument of the Digital Soul property right. The Residential AI Gateway Device installed in a Colorado residence is the physical instrument through which the resident exercises their Digital Soul property rights within the home. The resident's RAGD configuration rights are an extension of their Digital Soul property rights under this article and are inalienable.

(2) Physical mechanical override — inalienable right. Every Colorado resident in whose residence a RAGD is installed has the inalienable right to engage the RAGD's physical mechanical override at any time, for any reason, without notice, without explanation, and without consequence:

(a) Engaging the physical mechanical override instantly and completely severs all covered device network connectivity at the residential network perimeter — no covered device in the residence can transmit or receive data through any channel controlled by the RAGD;

(b) No covered operator, state agency, court order, or any other authority may require a resident to disengage the physical mechanical override, penalize a resident for engaging it, condition any service or benefit on the resident's agreement not to engage it, or remotely disable or circumvent it;

(c) The physical mechanical override is hardwired — it operates through physical circuit interruption, not software — ensuring that no firmware update, remote command, network signal, or software exploit can defeat it; and

(d) Engaging the physical mechanical override does not suspend, reduce, or affect the resident's Master Deed registration, Base Dividend entitlement, Premium Royalty accrual, or any other right under this article or title 24, article 20 — the resident's rights continue to accrue during any period of override engagement.

(3) Joint Household Consent architecture. For residences occupied by more than one adult Colorado resident:

(a) The RAGD's Joint Household Consent Interface allows each adult resident to register independent consent preferences for each covered device and each covered operator operating through the RAGD;

(b) The RAGD enforces the most restrictive consent setting among all adult residents for any given covered device or covered operator — if one adult resident has restricted a covered operator's access, that restriction applies to all network traffic through the RAGD regardless of other residents' settings;

(c) No adult resident's consent preferences may be modified by another resident — each adult resident's settings are independently authenticated through their individual Master Deed credential;

(d) A covered operator seeking to change the consent settings applicable to a residence must obtain affirmative consent from every adult resident independently — bundled consent, default-on consent, and implied consent are prohibited at the household level; and

(e) The physical mechanical override may be engaged by any adult resident independently — one resident's decision to engage the override protects the entire household, regardless of other residents' preferences.

(4) RAGD configuration rights — resident control. The resident's RAGD configuration rights include:

(a) The right to set individual consent permissions for each covered device and covered operator at any level of granularity — by data category, by time period, by purpose, or by blanket permission or restriction;

(b) The right to access the RAGD's local encrypted network log through the Universal Telemetry Allowance at any time — seeing a complete record of all covered device network activity within the residence;

(c) The right to configure the RAGD to activate the Non-Networked Isolation Protocol automatically based on time schedules, device behavior triggers, or network anomaly detection;

(d) The right to designate specific rooms, spaces, or times as Non-Networked Zones within the residence — areas where the RAGD enforces complete covered device connectivity severance regardless of device-level settings; and

(e) The right to receive plain-language real-time notifications through the myColorado platform or the RAGD's local interface when any Synthetic Data Integrity Marker trigger or Hash-Sentinel anomaly is detected within the residence — without any raw data leaving the home.

(5) Home as digital sanctuary — no warrantless RAGD access. The RAGD, its local network log, and all data processed by the RAGD within the residence are entitled to the full home sanctuary protections of the Fourth Amendment to the United States Constitution and Article II, Section 7 of the Colorado Constitution. The home's digital perimeter — as enforced by the RAGD — is the digital equivalent of the physical threshold of the home, crossing which requires a warrant. No government agency, law enforcement body, covered operator, or third party may access the RAGD's local log, query the RAGD's settings, or obtain any information about the RAGD's operation within the residence except pursuant to a warrant meeting the requirements of §10-10-303(5), served on the ODO through the Colorado Trust of Unique and Identifying Information — not on the covered operator and not on the RAGD directly.

RAGD ARCHITECTURAL SUMMARY — CONSTITUTIONAL DEFENSIBILITY ANALYSIS

Element	Design Feature	Constitutional Problem Solved	Strategic Effect
Perimeter regulation not device regulation	RAGD sits between ISP and home network — all foreign devices comply automatically by routing through it	Dormant Commerce Clause — state cannot regulate design of foreign-manufactured goods; can regulate utility access within state	No fight with Apple, Samsung, or Huawei about hardware redesign. They just have to route through the meter box. Every AI device on earth becomes instantly compliant.
Edge-computed compliance	Synthetic Data Integrity Markers and Hash-Sentinels processed locally — only cryptographic violation alerts transmitted, never raw data	Fourth Amendment smart meter concern — Naperville held granular home data transmission is a search. No raw data leaves = no search	Raw residential behavior stays in the home. The CCPAME knows a violation occurred — not what caused it. Law enforcement cannot mine RAGD data for behavioral surveillance.
Violation-alert-only transmission	Alert contains only: timestamp, device hash, violation category code, cryptographic proof — nothing else transmitted	Minimization requirement — any surveillance system must collect no more than necessary. Four data points is the minimum necessary for enforcement	Even with a warrant, the Trust only has four data points per alert. There is nothing else to produce. The architecture makes mass surveillance technically impossible.
Physical mechanical override	Hardwired circuit interruption — no software,	Griswold penumbra — the home has a zone of privacy that government cannot	No one can turn the resident's home network back on remotely. Not the operator. Not the

	no remote defeat, no operator override	penetrate; physical override is the resident's absolute control of that zone	government. Not a court order. The switch is physical. Physics is the law.
30-day symmetrical notice	30 days operator-to-resident before installation; 30 days operator-to-cure after ODO notice	Due process — adequate notice before enforcement; symmetry prevents government from giving residents less notice than operators receive	Equal notice both ways. Operators cannot ambush residents with installation. ODO cannot sanction operators without a cure window. Balanced, defensible, fair.
Import compliance pathway	Foreign devices comply through routing, not redesign — Prohibited Circumvention Device classification for deliberate bypass	Supremacy Clause and WTO — state cannot mandate foreign product redesign; can prohibit circumvention of domestic utility infrastructure	Every AI device in the world is either compliant by default (routes through RAGD) or a prohibited circumvention device. There is no middle ground and no foreign-manufacturer carve-out.

AMPLIFY Act v28 — §10-10-305 Residential AI Gateway Device · §15-15-165 Home Sanctuary Gateway Rights Civic Utility Perimeter Infrastructure · Edge-Computed Compliance · Physical Mechanical Override · Joint Household Consent · 30-Day Symmetrical Notice · Import Compliance Pathway

AMPLIFY ACT v28 — BILL 1 RESILIENCE & EXPANSION SECTIONS

§§15-15-165 through 15-15-168

Definitional Expansion · Neural Interface Pre-Classification · Operator Exit & Wind-Down · Bankruptcy Proofing & Digital Soul Asset Immunity

---

SECTION 15-15-165. SELF-EXECUTING DEFINITIONAL EXPANSION — TECHNOLOGY-NEUTRAL DIGITAL SOUL CLASSIFICATION — CCPAME CLASSIFICATION AUTHORITY

15-15-165. Self-executing definitional expansion — CCPAME classification authority — technology-neutral Digital Soul coverage — neural interface, ambient computing, and emerging data type pre-classification — legislative amendment not required.

(1) Legislative finding. The general assembly finds that: (a) Technology evolves faster than legislative cycles — a definitional framework requiring legislative amendment to capture each new category of resident data will be chronically behind the technology it governs; (b) The essential characteristic of Digital Soul data is not the specific technology through which it is generated but its function — uniquely identifying, profiling, or deriving commercial value from a Colorado resident's biological, behavioral, cognitive, or social existence; (c) A self-executing classification mechanism administered by the CCPAME preserves the legislative intent of the Digital Soul property right across all future technological development without requiring legislative action for each new data category; and (d) Pre-classification of foreseeable data categories — neural interface data, ambient computing data, synthetic biology data, spatial computing data — before those technologies achieve mass market

penetration closes the regulatory capture window that currently exists between technology deployment and legislative response.

(2) Self-executing classification mechanism. Any category of data not expressly enumerated in §15-15-101(1) automatically falls within the Digital Soul definition upon CCPAME classification. The CCPAME classification process:

(a) Is initiated by: (I) CCPAME Board motion; (II) petition by not fewer than one thousand (1,000) registered Master Deed holders; (III) referral by the ODO upon detection of new data categories being processed by covered operators; or (IV) petition by any covered operator seeking classification clarity before deploying a new data product;

(b) Requires: (I) publication of a proposed classification notice on the Public Accountability Dashboard; (II) a thirty (30) day public comment period; (III) a public hearing before the CCPAME Board; and (IV) a final classification determination published within sixty (60) days of the comment period close;

(c) Takes effect ninety (90) days after final publication — giving covered operators operating in the new data category time to implement compliance before the classification is operative; and

(d) Is subject to judicial review as a final agency action — but does not require legislative ratification. The general assembly has delegated this classification authority to the CCPAME as a condition of the technology-neutral regulatory framework established in this act.

(3) Pre-classified emerging data categories. The following data categories are hereby pre-classified as Digital Soul at the Protection Tier specified, effective upon the first commercial deployment of devices or systems generating such data to Colorado residents — without requiring any further CCPAME classification action:

(a) Neural interface data — Protection Tier 1 (highest). Data generated by any device interfacing directly with the human nervous system, including electroencephalographic data, electrocorticographic data, peripheral neural signal data, motor intent data, sensory feedback data, cognitive state data, attention and emotional state inferences, and any data derived from direct measurement of neural activity. Neural interface data is the most intimate category of Digital Soul — it is the resident's cognition itself. No covered operator may process neural interface data without: affirmative informed written consent renewed every ninety (90) days; a Neural Interface Data Processing Agreement approved by the ODO; and a Tier 1 Decentralized Identity Verification Protocol handshake for each data collection session. Neural interface data may never be used for advertising targeting, political profiling, employment screening, insurance underwriting, or law enforcement purposes — regardless of consent.

(b) Ambient computing data — Protection Tier 2. Data generated by always-on environmental computing systems — smart speakers, smart displays, ambient sensors, spatial computing headsets, mixed reality devices — including room audio, visual scene data, occupancy patterns, gesture data, gaze tracking, and environmental inference data;

(c) Synthetic biology and genetic interface data — Protection Tier 1. Data generated by direct-to-consumer genetic sequencing, microbiome analysis, proteomics, or any other molecular biology assay uniquely identifying or profiling the resident's biological characteristics — including raw sequence data, variant calls, ancestry inferences, health risk inferences, and pharmacogenomic profiles;

(d) Spatial computing and digital twin data — Protection Tier 2. Three-dimensional behavioral, positional, and interaction data generated by spatial computing devices, including room mapping data, object interaction data, physical movement patterns, and any digital twin or avatar representation derived from the resident's physical presence and behavior; and

(e) Autonomous vehicle and transportation AI data — Protection Tier 2. Behavioral, biometric, and route data generated by autonomous vehicle systems, including occupant identification data, behavioral patterns within the vehicle, route history, and inferred destination and activity patterns.

(4) Operator notice obligation. A covered operator that begins processing a new category of resident data — whether or not that category has been classified by the CCPAME — shall notify the ODO within thirty (30) days of the first Colorado resident data collection event in that category. The ODO shall evaluate the new category for classification under subsection (2) within sixty (60) days of notification.

SECTION 15-15-166. OPERATOR EXIT AND WIND-DOWN PROTOCOL — DIGITAL SOUL DATA DISPOSITION ON OPERATOR INSOLVENCY, ACQUISITION, OR EXIT — BANKRUPTCY TREATMENT — FOREIGN ACQUISITION RESTRICTION

15-15-166. Covered operator exit and wind-down — mandatory Digital Soul data disposition — resident election — Trust transfer as default — bankruptcy treatment — Digital Soul data not an asset of the bankruptcy estate — foreign acquisition restriction — successor operator obligations.

(1) Legislative finding. The general assembly finds that: (a) Covered operator insolvency, acquisition, or voluntary exit from the Colorado market creates a critical vulnerability — resident Digital Soul data held by the exiting operator may be transferred to a bankruptcy trustee, acquired by a successor entity, sold to a foreign operator, or simply abandoned without resident notification or consent; (b) Resident Digital Soul data is the resident's inalienable personal property — it is not an asset of the covered operator and may never be treated as such in any corporate transaction, insolvency proceeding, or regulatory action; (c) A mandatory wind-down protocol — triggered by any covered operator exit event — ensures that resident Digital Soul data exits with the resident, not with the operator; and (d) The risk that a foreign-government-affiliated entity could acquire a covered operator's Colorado resident Digital Soul data holdings is a direct threat to the security of the Colorado Trust of Unique and Identifying Information and is expressly prohibited.

(2) Operator exit events — trigger conditions. An Operator Exit Event occurs upon: (a) Filing of a voluntary or involuntary bankruptcy petition by or against the covered operator in any jurisdiction; (b) Assignment for the benefit of creditors; (c) Appointment of a receiver or liquidating trustee; (d) Voluntary cessation of covered operator services to Colorado residents; (e) Merger, acquisition, or change of control of the covered operator where the

acquiring entity is not a certified covered operator; (f) Acquisition of the covered operator by any entity in which a foreign government holds greater than ten percent (10%) ownership or control; or (g) Revocation of the covered operator's registration by the CCPAME.

(3) Mandatory resident notification. Within thirty (30) days of an Operator Exit Event: (a) The covered operator or its successor — or, if the operator is insolvent and has abandoned operations, the CCPAME acting on the operator's behalf — shall transmit a plain-language notification to every affected registered Master Deed holder; (b) The notification shall identify: the nature of the exit event; the categories of Digital Soul data held; the resident's three election options under subsection (4); the election deadline; and the default outcome if no election is made; and (c) The CCPAME shall publish a public notice on the Public Accountability Dashboard identifying the exiting operator and the number of affected Master Deed holders — without identifying individual residents.

(4) Resident election — three options. Upon receiving exit notification, each registered Master Deed holder shall elect one of the following within sixty (60) days: (a) Trust Transfer — the resident's Digital Soul data is transferred to the Colorado Trust of Unique and Identifying Information for the resident's account, to be held until the resident designates a successor certified covered operator; (b) Successor Operator Transfer — the resident designates a certified covered operator to receive their Digital Soul data directly, subject to a new Decentralized Identity Verification Protocol consent; or (c) Certified Deletion — the resident's Digital Soul data is permanently deleted by the exiting operator with cryptographic proof of deletion provided to the resident and logged in the Trust. If no election is made within sixty (60) days, Trust Transfer is the automatic default. Under no circumstances may resident Digital Soul data remain with the exiting operator, its bankruptcy estate, its trustee, or any uncertified successor beyond ninety (90) days of the Operator Exit Event.

(5) Bankruptcy treatment — Digital Soul data is not an asset of the estate. Notwithstanding any provision of the United States Bankruptcy Code, 11 U.S.C. §101 et seq., or any state insolvency law: (a) Resident Digital Soul data held by a covered operator in bankruptcy is not property of the bankruptcy estate under 11 U.S.C. §541 — it is the inalienable personal property of the resident and may not be administered, sold, transferred, or otherwise dealt with by the bankruptcy trustee; (b) The bankruptcy trustee's sole obligation regarding resident Digital Soul data is to facilitate the resident election process under subsection (4) within the required timeframes and to fund the CCPAME's assumption of notification obligations from available estate assets as a Tier 1 administrative expense; (c) Any sale of the covered operator's business, assets, or technology platform shall expressly exclude resident Digital Soul data — no sale order, plan of reorganization, or asset purchase agreement may purport to transfer resident Digital Soul data to any purchaser; and (d) The CCPAME shall file a notice of appearance and objection in any Colorado-connected bankruptcy proceeding involving a covered operator to enforce these provisions as a matter of state public policy.

(6) Foreign acquisition restriction. A covered operator whose ownership or control is acquired — in whole or in part — by any entity in which a foreign government, sovereign wealth fund, state-owned enterprise, or foreign military or intelligence agency holds greater than ten percent (10%) direct or indirect ownership or control: (a) Must notify the CCPAME within thirty (30) days of the acquisition closing; (b) Is automatically placed on a sixty (60) day probationary review during which the CCPAME assesses the national security implications of the foreign ownership for Colorado resident Digital Soul data security; (c) Shall not transfer any Colorado resident Digital Soul data to any system under foreign government control during the probationary review; and (d) If the CCPAME determines that the foreign acquisition presents an unacceptable security risk, the covered operator's

registration is revoked and an Operator Exit Event is triggered under subsection (2)(f) — the CCPAME notifies the Colorado Attorney General and refers the matter to the U.S. Department of Justice and the Committee on Foreign Investment in the United States (CFIUS).

SECTION 15-15-167. DIGITAL SOUL ASSET IMMUNITY — RESIDENT AUTOMATED MITIGATION ACCOUNT BANKRUPTCY EXEMPTION — JUDGMENT CREDITOR RESTRICTION — SELF-SETTLED TRUST INAPPLICABILITY

15-15-167. Digital Soul property immunity — Resident Automated Mitigation Account exemption from bankruptcy estate — exemption from judgment creditor claims — self-settled trust inapplicability — Colorado constitutional property protection — federal preemption savings.

(1) Legislative finding. The general assembly finds that: (a) The Resident Automated Mitigation Account represents the resident's return on their inalienable Digital Soul property right — it is not a government benefit, not a gratuitous transfer, and not a voluntary retirement contribution; it is the resident's earned property return; (b) Treating the Resident Automated Mitigation Account as available to creditors would perversely punish residents for exercising their Digital Soul property rights — the more valuable the resident's Digital Soul, the greater their liability exposure to creditors if the account is not protected; (c) Colorado's homestead exemption, vehicle exemption, and retirement account exemption all reflect the same policy: residents need a protected economic base to rebuild after financial adversity; the Resident Automated Mitigation Account is the digital-era equivalent of that protected base; and (d) The Digital Soul property right is inalienable — an inalienable property right that is available to creditors is not actually inalienable.

(2) Bankruptcy exemption. The Resident Automated Mitigation Account — including all accrued Base Dividends, Premium Royalties, UFIPA Income Distributions, Resident Mitigation Dividend payments, and investment returns — is exempt from inclusion in the bankruptcy estate under 11 U.S.C. §541 to the maximum extent permitted by Colorado's opt-out from the federal bankruptcy exemptions under C.R.S. §13-54-107. The exemption is: (a) Unlimited in amount — there is no dollar cap on the Resident Automated Mitigation Account bankruptcy exemption; (b) Available in both Chapter 7 and Chapter 13 proceedings; (c) Not waivable — a resident may not waive the exemption by contract, consent, or any other means; and (d) Applicable to all distributions pending at the date of the bankruptcy petition, not just the account balance.

(3) Judgment creditor restriction. No judgment creditor — including any state or federal agency, private creditor, or child support enforcement agency — may: (a) Garnish, levy, attach, or execute against the Resident Automated Mitigation Account; (b) Require the CCPAME to redirect any distribution from the Resident Automated Mitigation Account to a creditor; or (c) Treat the Resident Automated Mitigation Account balance as income for purposes of calculating a judgment debtor's ability to pay — except that child support arrears may be satisfied from the account upon a specific court order, limited to fifty percent

(50%) of any single distribution and not reducible below the resident's minimum subsistence distribution.

(4) Self-settled trust inapplicability. The Resident Automated Mitigation Account is not a self-settled trust under C.R.S. §38-10-111 or any other provision of Colorado trust law — it is a statutory property account holding the resident's earned property return. The self-settled trust exception to the Colorado exemption statutes does not apply. The CCPAME shall defend this characterization in any proceeding in which a creditor challenges the account's exempt status.

SECTION 15-15-168. SUPERMAJORITY AMENDMENT REQUIREMENT — CORE PROVISION PROTECTION — STATUTORY ENTRENCHMENT PENDING CONSTITUTIONAL RATIFICATION

15-15-168. Supermajority amendment requirement — two-thirds vote of both chambers required to amend core Digital Soul property right, distribution architecture, enforcement matrix, or Trust structure — protection pending Phase 2 constitutional ratification — rationale.

(1) Legislative finding. The general assembly finds that: (a) Simple majority amendment of this act's core provisions — the Digital Soul property right, the distribution architecture, the enforcement matrix, the CAMT structure, and the sweep prohibition — would expose the entire system to politically motivated raids during the period between Phase 1 enactment and Phase 2 constitutional ratification; (b) A supermajority amendment requirement for core provisions is a standard legislative entrenchment mechanism used in Colorado for constitutional implementing legislation and is within the power of one general assembly to impose on subsequent general assemblies as a rule of procedure; and (c) The supermajority requirement is self-repealing upon ratification of Article XXIX-A, after which constitutional amendment protection makes the statutory supermajority requirement unnecessary.

(2) Core provisions — supermajority required. A two-thirds vote of both the Colorado House of Representatives and the Colorado Senate is required to amend, repeal, or substantively modify: (a) The Digital Soul property right definition and inalienability provisions of §§15-15-101 through 15-15-110; (b) The distribution architecture — UFIPA Income Distribution, Resident Mitigation Dividend, and distribution percentages — of §§24-20-153 through 24-20-158; (c) The General Fund sweep prohibition of §24-20-157(9); (d) The Anti-Dilution Ratchet of §24-20-117; (e) The mandatory Investment Reserve floor of §24-20-154(2)(a); (f) The CAMT trust structure of §§24-20-150 through 24-20-157; (g) The enforcement matrix and Critical Severity Violation provisions of Annex E; (h) The AI Utility Property Privilege and Work Product Protection of §10-10-303; and (i) The Minor Digital Soul Trust provisions of §15-15-162.

(3) Self-repeal upon constitutional ratification. This section is automatically repealed upon certification by the Colorado Secretary of State that Article XXIX-A of the Colorado

Constitution has been ratified — at which point constitutional amendment protection makes the statutory supermajority requirement unnecessary and the general assembly returns to standard majority amendment authority for any remaining statutory implementing provisions.

AMPLIFY ACT v28 — BILLS 2 & 3 RESILIENCE & EXPANSION SECTIONS

§§10-10-305 through 10-10-306 · §§24-20-163 through 24-20-170

Quantum Cryptography · Open API · Anti-Concentration · Revenue Floor · Municipal Bonds · Infrastructure Investment · Cross-State Reciprocity · Workforce Transition · Premium Royalty Market

---

SECTION 10-10-305. CRYPTOGRAPHIC STANDARDS EMERGENCY UPGRADE AUTHORITY — POST-QUANTUM READINESS — TRUST INFRASTRUCTURE RESILIENCE

10-10-305. Cryptographic Standards Emergency Upgrade Authority — ODO authority to upgrade Trust cryptographic standards without legislative action — NIST post-quantum certification trigger — 90-day implementation mandate — covered operator upgrade obligation — legacy system sunset.

(1) Legislative finding. The general assembly finds that: (a) Current cryptographic standards — including those certified under FIPS 140-2 Level 3 — are vulnerable to quantum computing attacks that are projected to become operationally feasible within the operational lifespan of the Colorado Trust of Unique and Identifying Information; (b) NIST has published post-quantum cryptographic standards (FIPS 203, 204, 205) and will publish additional standards as the field develops; (c) Requiring legislative action to upgrade Trust cryptographic standards would create a window of vulnerability between NIST certification and legislative implementation that adversarial actors could exploit; and (d) The ODO must have standing authority to upgrade Trust cryptographic standards in response to NIST publications without awaiting legislative action — the same way the state upgrades software patches without legislative approval.

(2) Cryptographic Standards Emergency Upgrade Authority. The ODO has standing authority — without legislative action, CCPAME board vote, or executive order — to upgrade the cryptographic standards of the Colorado Trust of Unique and Identifying Information within ninety (90) days of NIST publishing any post-quantum cryptographic standard designated as applicable to sensitive government data systems. The upgrade authority: (a) Covers all cryptographic functions within the Trust — data encryption at rest, data encryption in transit, identity verification hash generation, session authentication, and digital signature standards; (b) Requires the ODO to publish a Cryptographic Upgrade Notice on the Public Accountability Dashboard simultaneously with the upgrade deployment; (c) Triggers a corresponding covered operator upgrade obligation — every certified covered operator must implement the upgraded cryptographic standards within one hundred eighty (180) days of the ODO's Cryptographic Upgrade Notice; and (d) Does not require the ODO to maintain backward compatibility with pre-upgrade standards beyond a twelve (12) month transition period.

(3) Quantum-resistant architecture mandate. Within thirty-six (36) months of enactment, the ODO shall: (a) Complete a full post-quantum readiness assessment of all Trust cryptographic infrastructure; (b) Publish a Post-Quantum Migration Plan on the Public Accountability Dashboard; (c) Implement hybrid classical-quantum resistant encryption for all Trust data at rest; and (d) Require all certified covered operators to certify post-quantum readiness as a condition of annual registration renewal beginning in the fourth year after enactment.

(4) Legacy system sunset. Any covered operator cryptographic system that has not been upgraded to current Trust cryptographic standards within twenty-four (24) months of a Cryptographic Upgrade Notice is automatically suspended from receiving new resident Decentralized Identity Verification Protocol consents until compliance is certified. Existing resident data held in non-compliant systems triggers an Operator Exit Event under §15-15-166 for the non-compliant data category.

SECTION 10-10-306. CCPAME OPEN API MANDATE — THIRD-PARTY DEVELOPER ECOSYSTEM — PUBLIC DATA ACCESSIBILITY — INNOVATION PLATFORM DESIGNATION

10-10-306. CCPAME Open API mandate — public data accessibility — third-party developer ecosystem — API certification — privacy-preserving data access — innovation platform designation — prohibited commercial exploitation.

(1) Open API mandate. Within twenty-four (24) months of enactment, the CCPAME and ODO shall publish and maintain open application programming interfaces (APIs) for the following public data systems: (a) The Public Accountability Dashboard — all publicly reported aggregate data in machine-readable format, updated in real time consistent with Dashboard update schedules; (b) The Legal Violation Pattern Database — anonymized aggregate violation data by category, geography, and actor type, updated quarterly; (c) The Environmental Impact Panel — aggregate energy consumption, renewable percentage, water consumption, and ORC output data, updated in real time; (d) The Civic Access Terminal network status — uptime, location, and accessibility status of all terminals, updated hourly; (e) The covered operator registry — name, registration status, industry classification, and compliance history of all registered covered operators; and (f) The Resident Data Cooperative registry — name, membership size, certification status, and collective negotiation outcomes of all certified cooperatives.

(2) API standards and certification. All CCPAME Open APIs shall: (a) Comply with REST or GraphQL architectural standards; (b) Provide data in JSON and CSV formats without proprietary encoding; (c) Require API key registration — free, available to any person or entity, with rate limits sufficient to support commercial application development; (d) Include complete technical documentation published on the CCPAME developer portal; and (e) Maintain ninety-nine percent (99%) uptime with a public status page showing real-time API availability.

(3) Third-party developer ecosystem. The CCPAME shall designate its public data infrastructure as an Innovation Platform and: (a) Publish annual developer challenges with

prize funding from Enterprise Mitigation Revenue — not to exceed one-tenth of one percent (0.1%) of annual revenue — for applications that increase resident benefit from the AMPLIFY Act ecosystem; (b) Maintain a public application registry where certified third-party developers list consumer applications built on CCPAME APIs; and (c) Certify third-party applications that meet privacy, security, and accuracy standards — certified applications may display a CCPAME Certified seal.

(4) Prohibited commercial exploitation. Third-party API access does not grant any right to: (a) Re-identify anonymized data; (b) Build commercial data products that compete with CCPAME core functions; (c) Use CCPAME data to target covered operators with competitive intelligence products; or (d) Access any resident-specific data — all API data is aggregate and anonymized. Violations result in permanent API access revocation and referral to the Colorado Attorney General.

SECTION 24-20-163. ANTI-CONCENTRATION RATE TRIGGER — DOMINANT MARKET OPERATOR DESIGNATION — MARKET STRUCTURE REVIEW — ATTORNEY GENERAL REFERRAL

24-20-163. Anti-concentration rate trigger — Dominant Market Operator designation — 35% Colorado-nexus token output threshold — 1.25x fee multiplier — 50% threshold market structure review — Attorney General antitrust referral — board conflict-of-interest enhanced restrictions.

(1) Legislative finding. The general assembly finds that extreme market concentration among covered operators creates regulatory capture risk — a single covered operator controlling the majority of Colorado-nexus AI output has disproportionate leverage to challenge fee structures, complicate compliance standards, and capture the CCPAME board through coordinated political pressure. An automatic rate multiplier triggered by concentration above defined thresholds creates a structural disincentive to monopolistic consolidation without requiring case-by-case regulatory action.

(2) Dominant Market Operator designation. A covered operator whose Colorado-nexus annual token output exceeds thirty-five percent (35%) of the total Colorado-nexus annual token output across all registered covered operators is automatically designated a Dominant Market Operator. Dominant Market Operator designation: (a) Triggers a 1.25x multiplier on all §24-20-156 base fee rates — applied to the Dominant Market Operator's full Colorado-nexus output, not just the portion exceeding the 35% threshold; (b) Triggers enhanced board conflict-of-interest restrictions — no person with any current or prior employment, ownership, consulting, or contractual relationship with the Dominant Market Operator or any of its affiliates within the prior five (5) years may serve on the CCPAME Board of Directors, the ODO Advisory Panel, or any CCPAME rate-setting committee; (c) Triggers a mandatory annual market structure report published on the Public Accountability Dashboard showing the operator's Colorado-nexus market share, fee contribution, and any changes in concentration; and (d) Is automatically removed when the operator's Colorado-nexus market share falls below 30% for two consecutive calendar years.

(3) 50% threshold — market structure review and AG referral. If any covered operator's Colorado-nexus annual token output exceeds fifty percent (50%) of total Colorado-nexus output: (a) The CCPAME shall initiate a mandatory Market Structure Review within sixty (60) days; (b) The CCPAME shall refer the market concentration data to the Colorado Attorney General for antitrust analysis under C.R.S. §6-4-101 et seq.; (c) The Attorney General shall respond within ninety (90) days with a determination whether to open an antitrust investigation; and (d) The 1.25x Dominant Market Operator multiplier increases to 1.5x for the period of the Market Structure Review and any subsequent antitrust investigation.

SECTION 24-20-164. ENTERPRISE MITIGATION REVENUE FLOOR GUARANTEE — AUTOMATIC RATE REVIEW TRIGGER — DYNAMIC ADJUSTMENT ACCELERATION — OPERATOR EXIT DETERRENCE

24-20-164. Enterprise Mitigation Revenue floor guarantee — 75% prior-year collection floor — automatic Dynamic Rate Adjustment Protocol acceleration trigger — CCPAME emergency rate review — revenue collapse deterrence — operator exit penalty.

(1) Revenue floor guarantee. If annual Enterprise Mitigation Revenue in any fiscal year falls below seventy-five percent (75%) of the prior fiscal year's total Enterprise Mitigation Revenue collections — whether due to operator exit, fee avoidance, revenue base erosion, or any other cause — the following automatic responses are triggered without CCPAME board action:

(a) The Dynamic Rate Adjustment Protocol under §24-20-156(4) activates immediately — not at the next annual cycle — and the CCPAME initiates an emergency rate review within thirty (30) days;

(b) The Mandatory Investment Reserve floor under §24-20-154(2)(a) is suspended for the affected fiscal year — the full Overflow Pool is available for Resident Mitigation Dividend distribution to maintain resident payment continuity;

(c) The CCPAME publishes a Revenue Shortfall Notice on the Public Accountability Dashboard within fifteen (15) days of detecting the shortfall, identifying the revenue gap and projected impact on resident distributions; and

(d) The Colorado Attorney General is automatically notified and shall investigate whether the revenue decline resulted from coordinated operator conduct constituting tortious interference with the CCPAME's revenue base or antitrust violations.

(2) Operator exit deterrence — exit penalty. A covered operator that voluntarily exits the Colorado market — ceasing all Colorado-nexus covered automation activity — within five (5) years of its first covered operator registration is subject to an Operator Exit Penalty: (a) Equal to fifty percent (50%) of the operator's average annual Enterprise Mitigation fee contribution over the period of its registration, multiplied by the number of years remaining in the five-year period; (b) Payable to the CAMT Investment Reserve within ninety (90) days of the exit event; (c) Collectible as a civil judgment in Colorado courts; and (d) Not applicable

to operators exiting due to insolvency under §15-15-166 — the exit penalty applies only to voluntary, solvent exits designed to avoid fee obligations.

SECTION 24-20-165. CCPAME REVENUE BOND AUTHORITY — MUNICIPAL BOND MARKET ACCESS — INFRASTRUCTURE CAPITAL — MARKET CONSTITUENCY CREATION

24-20-165. CCPAME revenue bond authority — Enterprise Mitigation Revenue-backed bonds — investment-grade rating mandate — permitted uses — bondholder protections — market constituency creation — General Fund non-recourse.

(1) Legislative finding. The general assembly finds that: (a) CCPAME revenue bond authority transforms the enterprise from a regulatory agency into a capital markets participant — investment banks, pension funds, and municipal bond investors become financially invested in CCPAME's revenue base, creating a powerful private-sector constituency defending Enterprise Mitigation Revenue against political erosion; (b) Revenue bonds backed by Enterprise Mitigation Revenue provide capital for infrastructure investment — Civic Access Terminal expansion, Trust infrastructure upgrades, ORC system financing, workforce transition programs — before revenue accumulates to fund those investments from cash flow; (c) CCPAME revenue bonds are not general obligation bonds — the State of Colorado's credit is not pledged and the General Fund bears no repayment obligation.

(2) Revenue bond authority. The CCPAME is authorized to issue revenue bonds, notes, and other obligations secured by a pledge of Enterprise Mitigation Revenue, subject to: (a) A maximum outstanding principal balance not exceeding thirty percent (30%) of the prior fiscal year's total Enterprise Mitigation Revenue; (b) A debt service coverage ratio covenant of not less than 1.5x — annual Enterprise Mitigation Revenue must exceed annual debt service by at least 50%; (c) Investment-grade rating from at least two nationally recognized statistical rating organizations before any bond issuance — the rating process is itself a public validation of the CCPAME's financial health; (d) A public bond issuance plan approved by the CCPAME Board of Directors and published on the Public Accountability Dashboard thirty (30) days before issuance; and (e) Proceeds restricted to permitted uses under subsection (3) — bond proceeds may not supplement operating revenues or fund resident distributions.

(3) Permitted bond uses. CCPAME revenue bond proceeds may be used exclusively for: (a) Civic Access Terminal network expansion and upgrade; (b) Colorado Trust of Unique and Identifying Information infrastructure construction, upgrade, and post-quantum cryptographic migration; (c) ORC thermal recapture system construction financing under §24-20-143; (d) Civic Enforcement Access Terminal network build-out; (e) Workforce Transition Account infrastructure under §24-20-169; and (f) Refinancing of outstanding CCPAME obligations at lower interest rates.

(4) General Fund non-recourse. CCPAME revenue bonds are payable solely from Enterprise Mitigation Revenue pledged to bond repayment. The State of Colorado, the

General Fund, and the Colorado Automation Mitigation Trust bear no liability for CCPAME revenue bond repayment. Bond documents shall prominently disclose this non-recourse character. No state official may pledge state credit to support CCPAME revenue bond repayment without a constitutional amendment.

SECTION 24-20-166. COLORADO INFRASTRUCTURE INVESTMENT AUTHORITY — INVESTMENT RESERVE DIRECT INVESTMENT — SOVEREIGN WEALTH FUND MODEL — DOUBLE RETURN ARCHITECTURE

24-20-166. Colorado Infrastructure Investment Authority — Investment Reserve direct investment in Colorado infrastructure — permitted infrastructure categories — return-generating requirements — UFIPA income stream integration — double return architecture — rural broadband priority.

(1) Legislative finding. The general assembly finds that: (a) The Investment Reserve currently holds exclusively financial instruments — bonds, treasuries, and income-producing securities; (b) Direct investment in Colorado infrastructure — rural broadband, water treatment, renewable energy, affordable housing — generates both financial returns flowing through the UFIPA pipeline to residents and direct service improvements serving those same residents; (c) Technology companies whose data extraction funds the Investment Reserve are the same companies whose infrastructure demands — power, water, connectivity — strain Colorado's public infrastructure; routing Investment Reserve returns into that infrastructure closes the loop between extraction and restoration; and (d) The Alaska Permanent Fund, Norway Government Pension Fund Global, and similar sovereign wealth funds have demonstrated that permanent endowment funds can generate superior long-term returns through diversified direct investment while maintaining liquidity for distributions.

(2) Direct infrastructure investment authority. The CCPAME Investment Committee — a subcommittee of the Board of Directors established under subsection (3) — may allocate up to twenty-five percent (25%) of the Investment Reserve to direct investment in Colorado infrastructure projects meeting the criteria of subsection (4). Infrastructure investments are treated as Investment Reserve principal for UFIPA purposes — their returns are Net Income Receipts flowing through §24-20-157 to residents as UFIPA Income Distributions.

(3) Investment Committee. The CCPAME Board shall establish an Investment Committee of not fewer than five (5) members including: (a) Not fewer than two (2) members with demonstrated professional investment management experience; (b) Not fewer than one (1) member with infrastructure finance experience; (c) Not fewer than one (1) member representing rural Colorado communities; and (d) Not fewer than one (1) registered Master Deed holder elected by the Master Deed holder population through a process administered by the Secretary of State. No CCPAME Board member with a conflict of interest in any investment under consideration may participate in the Investment Committee vote on that investment.

(4) Permitted infrastructure investment categories. The Investment Reserve may be directly invested in: (a) Rural broadband infrastructure — priority given to Colorado counties with less than 25 Mbps median download speed serving residential addresses; (b) Water treatment and conservation infrastructure — including advanced metering, recycled water systems, and agricultural water efficiency projects — priority given to projects in watersheds affected by covered compute facility water consumption under §24-20-150; (c) Renewable energy generation and storage — solar, wind, geothermal, and pumped hydro projects with a minimum 20-year power purchase agreement with a Colorado utility or municipal power authority; (d) Affordable housing construction and preservation — projects meeting HUD affordability standards in Colorado communities where covered compute facility presence has increased housing cost burdens; and (e) Public transit infrastructure in communities with major covered compute facility concentrations — reducing the transportation externality of large-scale employment centers that do not provide adequate transit access.

(5) Return requirement. Every direct infrastructure investment must: (a) Generate a projected annual return of not less than the Investment Reserve's current blended yield on financial instruments — direct investment must not dilute the Investment Reserve's income-generating performance; (b) Be structured as a loan, equity investment, or revenue participation — not a grant; and (c) Include a liquidation pathway — the Investment Committee must be able to exit each direct investment within a five-year horizon if required to meet distribution obligations.

SECTION 24-20-167. CROSS-STATE DIGITAL PROPERTY RIGHTS RECIPROCITY — COLORADO STANDARD AS NATIONAL BASELINE — RECIPROCITY CERTIFICATION — MULTI-STATE MASTER DEED RECOGNITION

24-20-167. Cross-state digital property rights reciprocity — CCPAME equivalency certification — Colorado standard as national baseline — mutual Master Deed recognition — reciprocating state resident protections in Colorado — Colorado resident protections in reciprocating states — interstate commerce nexus.

(1) Legislative finding. The general assembly finds that: (a) Colorado is the most advanced digital property rights jurisdiction in the United States and has an opportunity to export its regulatory architecture to other states — establishing Colorado's framework as the de facto national standard before federal legislation preempts state innovation; (b) A reciprocity framework that requires other states to meet Colorado's standard for equivalency certification gives Colorado permanent leverage in the development of national digital property rights norms — states that want Colorado reciprocity must match Colorado's protections; (c) Multi-state Master Deed recognition eliminates the barrier to registration for Colorado residents who also reside or work in other states, and attracts out-of-state residents to register Colorado Master Deeds as the gold standard of digital property rights protection.

(2) CCPAME equivalency certification. The CCPAME shall establish an Interstate Digital Property Rights Equivalency Certification process evaluating other states' digital property

rights frameworks against the following minimum standards: (a) An inalienable digital property right in resident data with a definition at least as comprehensive as Colorado's Digital Soul definition; (b) A consent-based data collection framework functionally equivalent to the Decentralized Identity Verification Protocol; (c) An enterprise mitigation fee or equivalent revenue mechanism funding resident distributions; (d) A trust structure protecting distributions from government sweep equivalent to the CAMT's sweep prohibition; (e) An enforcement matrix with statutory damages equivalent to Colorado's Annex E; and (f) An independent administrative enterprise not subject to executive or legislative capture functionally equivalent to the CCPAME.

(3) Reciprocity effects upon certification. Upon CCPAME equivalency certification of a reciprocating state: (a) Colorado Master Deed registrations are recognized in the reciprocating state as equivalent to that state's resident registration — Colorado residents retain their full Colorado Digital Soul rights when their data is processed by covered operators in the reciprocating state; (b) Reciprocating state residents who register Colorado Master Deeds receive Colorado Digital Soul protections for data processed by Colorado-registered covered operators; (c) Covered operators registered in both Colorado and the reciprocating state may satisfy both states' compliance obligations through a unified filing submitted to both states' administrative enterprises; and (d) The CCPAME publishes a reciprocity status dashboard showing all certified reciprocating states and their equivalency scores relative to Colorado's standard.

(4) Colorado as national standard. The CCPAME shall: (a) Publish an annual National Digital Property Rights Index comparing all U.S. states' digital property rights frameworks against Colorado's standard; (b) Provide technical assistance to other states developing digital property rights legislation — at the requesting state's expense — using Colorado's framework as the template; (c) Participate in the National Conference of State Legislatures digital property rights working group as Colorado's designated representative; and (d) Notify the Colorado congressional delegation when any federal digital property rights legislation is proposed that would preempt Colorado's more protective framework — triggering the CCPAME's standing to appear in any federal legislative or regulatory proceeding affecting Colorado's Digital Soul framework.

SECTION 24-20-168. WORKFORCE TRANSITION ACCOUNT — AUTOMATION DISPLACEMENT RETRAINING — MASTER DEED HOLDER SKILLS ACCOUNT — 5% ENTERPRISE MITIGATION REVENUE ALLOCATION

24-20-168. Workforce Transition Account — automation displacement retraining — Master Deed holder skills account — 5% Enterprise Mitigation Revenue allocation — permitted uses — credential matching — employer co-investment — anti-duplication with existing state programs.

(1) Legislative finding. The general assembly finds that: (a) The covered automation activity taxed under this act is causing real and measurable workforce displacement in Colorado — the same revenue being collected from automation is the appropriate source of funding for

the workforce transition that automation is causing; (b) A Workforce Transition Account available to registered Master Deed holders converts displaced workers from opponents of automation — who currently see no benefit flowing to them — into stakeholders in the AMPLIFY Act ecosystem with a direct financial interest in the system's success; (c) A skills account funded from Enterprise Mitigation Revenue is qualitatively different from a cash distribution — it is an investment in the resident's future earning capacity, not a consumption transfer; and (d) Employer co-investment requirements ensure that covered operators who benefit from a skilled Colorado workforce contribute to workforce transition alongside the CCPAME.

(2) Workforce Transition Account — establishment. A Workforce Transition Account is established as a dedicated subaccount of the CAMT, funded at five percent (5%) of annual Enterprise Mitigation Revenue before the Overflow Pool is calculated — treated as a program account ahead of the resident distribution waterfall. The Workforce Transition Account: (a) Is administered by the CCPAME in coordination with the Colorado Department of Labor and Employment; (b) Is available to any registered Master Deed holder who: (I) has experienced documented automation-related job displacement in the prior twenty-four (24) months; (II) is currently employed in an occupation with a documented automation risk score above 0.7 on the Frey-Osborne or equivalent automation risk index; or (III) is a resident of a Colorado community where covered compute facility deployment has materially altered the local labor market; and (c) Provides each eligible resident with an annual Workforce Transition Credit of not less than five thousand dollars ($5,000) — scaled to documented displacement severity — deposited into the resident's Resident Automated Mitigation Account as a restricted skills account sub-balance.

(3) Permitted uses. Workforce Transition Credits may be used exclusively for: (a) Tuition and fees at any Colorado accredited institution of higher education, community college, or registered apprenticeship program; (b) Industry certification and credentialing programs in fields with documented Colorado labor demand; (c) Equipment and software required for credentialing programs; (d) Childcare costs directly enabling enrollment in qualifying programs — not to exceed thirty percent (30%) of the Workforce Transition Credit; and (e) Transportation costs directly enabling program attendance in rural communities — not to exceed fifteen percent (15%) of the Credit.

(4) Employer co-investment requirement. Any covered operator whose Colorado-nexus annual Enterprise Mitigation fee exceeds five million dollars ($5,000,000) must: (a) Publish an annual Colorado Workforce Transition Plan identifying the operator's projected automation-related workforce impacts in Colorado over the following three years; (b) Contribute to the Workforce Transition Account an amount equal to ten percent (10%) of its annual Enterprise Mitigation fee — in addition to the fee itself — as an employer co-investment; and (c) Preferentially consider Colorado residents with Workforce Transition Credits for open positions in the operator's Colorado operations that match the credentials being pursued. Employer co-investment contributions are credited against the operator's Enterprise Mitigation fee in subsequent years at a rate of fifty cents ($0.50) credit per dollar contributed — creating a direct financial incentive for operator participation.

SECTION 24-20-169. PREMIUM ROYALTY SECONDARY ASSIGNMENT MARKET — CCPAME-REGULATED

EXCHANGE — VOLUNTARY RESIDENT ASSIGNMENT — FLOOR PROTECTION — REVOCABILITY — PROHIBITED ASSIGNMENTS

24-20-169. Premium Royalty secondary assignment market — CCPAME-regulated voluntary exchange — maximum 49% assignment — statutory floor protection — 30-day revocability — prohibited assignment categories — anti-predatory assignment rules — resident economic agency.

(1) Legislative finding. The general assembly finds that: (a) Premium Royalty rights are the resident's earned property return from their Digital Soul — they are property rights that, like other property rights, should be usable as economic currency by the resident when the resident chooses; (b) A regulated secondary assignment market — with strong floor protections, mandatory revocability, and categorical prohibitions on predatory assignments — allows residents to use their Premium Royalty rights to access services they value while maintaining the systemic integrity of the resident distribution architecture; and (c) The assignment market is entirely voluntary — no resident may be required, pressured, or incentivized through service degradation to assign any portion of their Premium Royalty rights.

(2) Secondary assignment market. The CCPAME shall establish and regulate a Premium Royalty Secondary Assignment Market — a regulated exchange through which registered Master Deed holders may voluntarily assign a portion of their future Premium Royalty distributions to certified covered operators, certified cooperatives, or CCPAME-approved service providers in exchange for services, credits, or other consideration. The market operates under the following rules:

(a) Maximum assignment — no resident may assign more than forty-nine percent (49%) of their total Premium Royalty rights across all assignments combined — the resident retains at least 51% of their Premium Royalty regardless of the number or nature of assignments;

(b) Statutory floor protection — no assignment may reduce any single distribution below the statutory Base Dividend floor established in §15-15-110, as CPI-adjusted under §10-10-304(1);

(c) Mandatory 30-day revocability — every assignment is revocable by the resident at any time with thirty (30) days written notice — no assignment may include a lock-up period exceeding ninety (90) days, after which the revocability right is restored;

(d) Assignee certification — only CCPAME-certified assignees may receive Premium Royalty assignments — certification requires demonstration that the consideration offered is fair market value for the Premium Royalty assigned and that no predatory practices are employed; and

(e) CCPAME market oversight — the CCPAME monitors all assignment transactions in real time through the Secondary Assignment Market platform and may suspend any assignee whose practices indicate predatory assignment solicitation.

(3) Prohibited assignments. The following assignments are void and unenforceable regardless of resident consent: (a) Assignments made as a condition of employment, housing, credit, government benefit, or any other necessity of life; (b) Assignments made pursuant to any contract of adhesion or standard-form agreement presented without individualized negotiation opportunity; (c) Assignments to any entity under active CCPAME

enforcement action; (d) Assignments of more than six (6) months of future Premium Royalty distributions — the assignment term may not exceed six months, after which a new voluntary assignment must be executed; and (e) Assignments made under circumstances of documented financial distress — the CCPAME shall monitor for distress-driven assignment patterns and may impose a cooling-off period of thirty (30) days before a distress-flagged assignment takes effect.

v28 COMPLETE STRENGTHENING PROVISIONS — SINGLE-SUBJECT ANALYSIS AND GRAVITY IMPACT

Section	Provision	What It Does	Gravity Impact
§15-15-165	Definitional Expansion Clause	CCPAME classifies new data types without legislation — neural interface, ambient, synthetic biology, spatial computing pre-classified at Tier 1/2	Bill never becomes obsolete. Neural interface data captured before Neuralink ships. Technology evolves — bill evolves with it automatically.
§15-15-166	Operator Exit & Wind-Down	Digital Soul data not bankruptcy estate asset — resident election on exit — bankruptcy trustee may not sell resident data — foreign acquisition restriction — CFIUS referral	Closes the most dangerous gap. A Cloudflare-scale bankruptcy can no longer put 3M Colorado residents' Digital Soul on the auction block.
§15-15-167	Bankruptcy Proofing / Asset Immunity	RAMA fully exempt from bankruptcy estate — unlimited exemption — not waivable — judgment creditor restriction — self-settled trust inapplicability	Residents who need protection most — those in financial distress — keep their Digital Soul account intact. The property right is actually inalienable.
§15-15-168	Supermajority Amendment Requirement	2/3 both chambers to amend core provisions — Digital Soul right, distribution architecture, sweep prohibition, enforcement matrix — self-repeals on constitutional ratification	Makes the bill raid-resistant between Phase 1 and Phase 2. A hostile simple majority can't gut the system while the constitutional amendment is circulating.
§10-10-305	Quantum Cryptography Upgrade	ODO upgrades Trust crypto within 90 days of NIST post-quantum certification — no legislative action required — covered operator upgrade obligation — legacy system sunset	Trust stays secure regardless of what computing does. Post-quantum migration is automatic, not legislative.
§10-10-306	CCPAME Open API Mandate	Machine-readable public APIs for Dashboard, Pattern Database, Environmental Panel, operator registry — third-party developer ecosystem — innovation platform	Turns the bill into a platform. Tenant rights apps, wage theft detectors, police encounter analytics — built by developers, maintained by the ecosystem.
§24-20-163	Anti-Concentration Rate Trigger	35% market share = Dominant Market Operator, 1.25x fee multiplier — 50% threshold triggers AG antitrust referral — enhanced board conflict-of-interest rules	Consolidation becomes self-defeating. The bigger one operator gets, the more expensive Colorado becomes for them.
§24-20-164	Revenue Floor Guarantee	75% prior-year collections floor — automatic Dynamic Rate Adjustment acceleration — Investment Reserve floor suspended to protect resident payments — AG notified	Revenue can't collapse faster than the rate structure can respond. Resident checks are protected even during revenue disruption.

§24-20-165	Municipal Bond Authority	CCPAME revenue bonds backed by Enterprise Mitigation Revenue — 30% of prior year revenue cap — 1.5x debt service coverage — investment-grade rating mandate — General Fund non-recourse	Wall Street becomes a defender of Enterprise Mitigation Revenue. Bond ratings are independent public validation of the system's financial health.
§24-20-166	Infrastructure Investment Authority	Investment Reserve direct investment in rural broadband, water, renewable energy, affordable housing — sovereign wealth fund model — return requirement — double return architecture	Same revenue that mitigates automation externalities funds the infrastructure those externalities degrade. Double return: financial yield + direct service improvement.
§24-20-167	Cross-State Reciprocity	CCPAME certifies equivalent state frameworks — Colorado standard as minimum equivalency bar — multi-state Master Deed recognition — National Digital Property Rights Index	Colorado exports its architecture. Other states match Colorado's standard to get reciprocity. Colorado defines the national baseline.
§24-20-168	Workforce Transition Account	5% of Enterprise Mitigation Revenue — $5K minimum annual credit per eligible displaced worker — employer co-investment 10% of fee with 50-cent credit return — skills account not cash	Displaced workers become stakeholders. The companies automating them away fund their retraining. The system turns opponents into constituents.
§24-20-169	Premium Royalty Secondary Market	Voluntary assignment up to 49% — 30-day revocability always — 6-month term max — prohibited in employment/housing contexts — CCPAME-regulated exchange	Digital Soul property rights become economic currency residents can use while keeping control. The property right gains utility without losing protection.

AMPLIFY ACT v28 — FINAL PRIORITY SECTIONS

§§15-15-170 · 15-15-171 · 15-15-172 · 24-20-171

Voter Data Sovereignty · DNA & Genetic Data Absolute Protection · Quantum Infrastructure Emergency Funding

The state owns the tally. The voter owns the vote. — Voter data, DNA, and quantum security are the three highest-priority protections in this act.

SECTION 15-15-170. VOTER DATA SOVEREIGNTY — THE STATE OWNS THE TALLY — THE VOTER OWNS THE VOTE — VOTER DIGITAL SOUL ABSOLUTE PROTECTION — POLITICAL DATA OPERATOR PROHIBITION

15-15-170. Voter Data Sovereignty — separation of tally from voter — voter's ballot, registration data, voting history, precinct behavioral data, and political profile data are inalienable Digital Soul — state's lawful interest limited to aggregate tally — covered political data operators prohibited — AI-assisted voter targeting — absolute consent requirement — Fourteenth Amendment equal protection foundation.

(1) Legislative findings. The general assembly finds and declares that:

(a) The right to vote is the foundational right of democratic self-governance — and the data generated by the exercise of that right belongs to the voter, not to the state, not to any political party, not to any campaign, not to any data broker, and not to any covered operator processing that data for commercial or political advantage;

(b) There is a precise and legally significant distinction between: (I) the TALLY — the aggregate count of votes cast for each candidate or measure, which is a public governmental record belonging to the People of Colorado collectively; and (II) the VOTE — the individual voter's registration data, party affiliation, voting history, precinct assignment, absentee ballot status, signature data, demographic profile, behavioral data generated through the voting process, and any political preference or behavior data derived from that voter's participation — which is the voter's inalienable Digital Soul at the highest tier of protection;

(c) The commercial political data industry — including voter file vendors, political analytics platforms, campaign technology providers, microtargeting services, and AI-assisted voter persuasion systems — processes Colorado voter data at industrial scale for commercial and political advantage, generating revenue from the voter's most intimate democratic expression without the voter's meaningful consent and without returning any value to the voter;

(d) AI-assisted voter targeting — the use of machine learning models trained on voter behavioral data to predict, influence, and manipulate individual voting decisions — represents a qualitatively different threat to democratic self-governance than traditional mass advertising, because it operates at the individual level, in real time, with a precision that the individual voter cannot detect or counter;

(e) The voter's Digital Soul data generated through electoral participation is not merely personal property — it is the data substrate of democratic self-governance itself; its commercialization without consent is an injury not just to the individual voter but to the democratic process; and

(f) Voter Data Sovereignty — the principle that the state's lawful interest in electoral data is limited to the aggregate tally, and that all individual voter data belongs to the voter as inalienable Digital Soul — is the digital-era expression of the secret ballot principle established in Colorado law since 1891.

(2) Definitional framework — Voter Digital Soul. For purposes of this section:

(a) 'Voter Digital Soul' means all data uniquely identifying, profiling, or derived from an individual Colorado registered voter's participation in the electoral process, including: (I) voter registration data — name, address, party affiliation, registration date, registration status; (II) voting history — whether the voter voted in each election, by what method (in-person, mail, early), at what location; (III) ballot request and return data — absentee ballot request dates, return dates, cure status; (IV) signature data collected through the ballot process; (V) precinct assignment and geographic electoral unit data; (VI) demographic data collected or inferred through the voter registration process; (VII) any behavioral data generated through government-operated voter registration portals, election websites, or voting systems; and (VIII) any political preference, party support, candidate preference, issue position, or electoral behavior data derived or inferred from any of the above through any analytical process;

(b) 'Political Data Operator' means any covered operator that processes Voter Digital Soul data for commercial, political, or analytical purposes — including voter file vendors, political analytics platforms, campaign technology providers, voter contact systems,

microtargeting services, AI-assisted voter persuasion systems, and any operator whose covered automation activity includes training models on or generating inferences from Voter Digital Soul data; and

(c) 'State Electoral Tally' means the aggregate count of votes cast for each candidate or ballot measure in each Colorado election — a public governmental record that belongs to the People of Colorado collectively, is subject to public inspection under C.R.S. §24-72-204, and is expressly excluded from Voter Digital Soul.

(3) Voter Digital Soul — inalienable property right at highest protection tier. Voter Digital Soul is the voter's inalienable intangible personal property at Protection Tier 1 — the highest tier under this act — with the following specific attributes:

(a) The voter's Voter Digital Soul may not be processed, sold, transferred, licensed, or used by any political data operator without the voter's affirmative, informed, specific, written consent — a blanket consent to voter file access is not sufficient; consent must specify the exact data categories, the specific operator, the specific electoral purpose, and the specific time period, and must be renewed before each election cycle;

(b) The voter's Voter Digital Soul may not be used for AI-assisted voter targeting, microtargeting, persuasion modeling, sentiment analysis, or any other automated individual-level political influence activity regardless of consent — this prohibition is absolute and is not subject to waiver;

(c) The voter's party affiliation data, candidate preference data, and issue position data derived from Voter Digital Soul processing may not be sold, licensed, or transferred to any third party regardless of consent — these categories are non-transferable;

(d) The voter has a Universal Telemetry Allowance over all Voter Digital Soul data — including all data held by political data operators and the Colorado Secretary of State's voter registration system — with the same uncapped access rights established in §24-20-158; and

(e) A voter's Master Deed registration automatically encompasses their Voter Digital Soul — no separate registration or separate consent framework is required. Voter Digital Soul protection is an automatic attribute of Master Deed registration.

(4) State's lawful electoral data interest — limited to aggregate tally. The State of Colorado's lawful interest in electoral data is limited to:

(a) The State Electoral Tally — aggregate vote counts for each candidate and measure, public record;

(b) The minimum voter registration data required to administer elections under C.R.S. §1-2-101 et seq. — held exclusively by the Secretary of State and county clerks for electoral administration purposes, not subject to commercial disclosure;

(c) Signature verification data — used exclusively for ballot cure processes under C.R.S. §1-7.5-107.3, not retainable beyond the applicable election canvass period; and

(d) Voter roll maintenance data — used exclusively for list maintenance under the National Voter Registration Act, 52 U.S.C. §20507, not subject to commercial disclosure.

The state may not sell, license, or provide bulk access to voter registration data for commercial or political purposes — any existing Colorado statute permitting voter file access to political parties, campaigns, or commercial vendors is superseded by this section to the extent it conflicts with the protections herein.

(5) Political Data Operator obligations — Voter Digital Soul. A political data operator shall:

(a) Register with the CCPAME as a covered operator in the Political Data Operations industry classification — subject to the statutory rate schedule in §24-20-156, with a Political Data Operations Premium of 1.5x applied to all base fee rates reflecting the heightened democratic harm of commercial voter data processing;

(b) Cease all processing of Colorado Voter Digital Soul within ninety (90) days of this act's effective date for any voter who has not provided compliant consent under subsection (3)(a) — and certify compliance to the ODO with cryptographic proof of data deletion for non-consenting voters;

(c) Provide each Colorado voter with a Voter Digital Soul Transparency Report annually — identifying all Voter Digital Soul data held, all processing performed, all third parties to whom data was transferred, and the specific consent basis for each;

(d) Maintain a publicly accessible Voter Digital Soul Registry on the CCPAME Public Accountability Dashboard showing — without individual identification — the aggregate categories of Voter Digital Soul processed, the number of Colorado voters covered, and the Enterprise Mitigation fees assessed; and

(e) Never, under any circumstances, use Voter Digital Soul data to train AI models for individual-level voter targeting, political persuasion, or electoral outcome prediction — this prohibition survives the expiration or revocation of any consent and applies regardless of the form of AI model training.

(6) AI-assisted voter targeting — absolute prohibition. No person, political data operator, political campaign, political party, political action committee, independent expenditure committee, or any other entity may:

(a) Use any AI model, machine learning system, or automated analytical tool trained on Colorado Voter Digital Soul data to generate individual-level voter targeting, persuasion, or mobilization recommendations;

(b) Purchase, license, or receive any AI-generated individual voter targeting product derived from Colorado Voter Digital Soul data;

(c) Deploy any AI-assisted communication system that uses Colorado Voter Digital Soul to personalize political messaging at the individual voter level; or

(d) Use covered operator AI systems to generate synthetic media — deepfakes, voice synthesis, AI-generated images — depicting any Colorado candidate, elected official, or voter in any electoral context without affirmative disclosure of AI generation meeting the standards of C.R.S. §1-13-109 (Colorado's AI disclosure in political advertising statute).

Violation of subsection (6) is a Critical Severity Violation under Annex E and constitutes a Class 5 felony under C.R.S. §18-1.3-401 — the general assembly hereby amends the Colorado Criminal Code to add AI-assisted voter targeting using prohibited Voter Digital Soul data as a Class 5 felony, separate from any civil penalty under this act.

(7) Enforcement — statutory damages — qui tam provision. A Colorado registered voter whose Voter Digital Soul is processed in violation of this section is entitled to:

(a) Statutory damages of one thousand dollars ($1,000) per data record processed in violation, per day of noncompliance — payable directly to the voter's Resident Automated Mitigation Account;

(b) Actual damages, including but not limited to any political harm caused by AI-assisted targeting using the voter's data;

(c) Attorney fees and costs; and

(d) Injunctive relief including immediate cessation of all Voter Digital Soul processing and certified deletion of all Voter Digital Soul data held in violation.

Qui Tam provision: any Colorado resident who identifies and reports a violation of this section that results in a statutory damages award is entitled to fifteen percent (15%) of the damages collected — creating distributed enforcement by every Master Deed holder in the state.

SECTION 15-15-171. DNA AND GENETIC DATA ABSOLUTE PROTECTION — HIGHEST TIER DIGITAL SOUL — NON-WAIVABLE PROHIBITIONS — LAW ENFORCEMENT RESTRICTION — INSURANCE AND EMPLOYMENT BAR — FAMILIAL EXTENSION

15-15-171. DNA and genetic data as inalienable Digital Soul Protection Tier 1 — absolute prohibition on processing without express annual written consent — law enforcement genetic surveillance restriction — insurance and employment use bar — familial genetic data extension — ancestry service obligations — genetic data bankruptcy immunity — non-waivable.

(1) Legislative findings. The general assembly finds and declares that:

(a) DNA data is the most intimate category of Digital Soul — it is not merely data about the resident, it is the resident at the molecular level; it contains information about the resident's health, ancestry, predispositions, family relationships, and biological identity that cannot be changed, cannot be revoked, and cannot be protected retroactively once disclosed;

(b) Unlike all other categories of Digital Soul, DNA data affects not only the resident but all biological relatives — a resident's DNA discloses information about parents, siblings, children, and extended family members who have not consented to any disclosure; the property right in DNA data must therefore extend to protect the resident's biological family members' informational privacy as derivative beneficiaries;

(c) The commercial direct-to-consumer genetic testing industry — 23andMe, AncestryDNA, and successor services — has created databases containing the DNA of hundreds of millions of people, the full implications of which for insurance discrimination, employment discrimination, law enforcement surveillance, and foreign government access are not yet fully understood; the bankruptcy and data sale risks of these services, as demonstrated by 23andMe's 2025 bankruptcy and the resulting uncertainty over its genetic database, require statutory protection that travels with the data regardless of which entity holds it;

(d) Colorado's Genetic Information Privacy Act, C.R.S. §10-3-1104.7, provides baseline protection but does not address covered operator AI processing of genetic data, does not provide the property right framework established in this act, and does not address the familial extension of genetic privacy; this section supplements and strengthens existing Colorado genetic privacy law; and

(e) Genetic data is forever — the protections in this section must be permanent, non-waivable, and immune to corporate transaction, bankruptcy, or foreign acquisition.

(2) DNA and genetic data — Tier 1 absolute protection. DNA and genetic data — including raw genomic sequence data, processed variant calls, ancestry estimates, health risk inferences, pharmacogenomic profiles, and any other data derived from direct analysis of a resident's biological sample — is Digital Soul at Protection Tier 1 with the following absolute protections:

(a) No covered operator may collect, process, store, transfer, or use Colorado resident DNA or genetic data without: (I) affirmative, specific, written consent renewed annually; (II) a Genetic Data Processing Agreement approved by the ODO specifying the exact processing purpose, data retention period, and deletion protocol; and (III) a Tier 1 Decentralized Identity Verification Protocol handshake for each data collection event — not a blanket consent covering all future data collection;

(b) Consent to genetic data processing for one purpose — such as ancestry analysis — does not constitute consent to any other purpose — such as health risk assessment, law enforcement cooperation, research, or AI model training; each purpose requires independent consent;

(c) A resident may revoke consent to genetic data processing at any time with immediate effect — revocation triggers a mandatory deletion obligation within thirty (30) days with cryptographic proof of deletion provided to the resident and logged in the Trust; and

(d) These protections are non-waivable — no contract, terms of service, employment agreement, insurance application, or any other instrument may require a resident to waive genetic data protection as a condition of any benefit, service, employment, or insurance.

(3) Absolute prohibitions — non-waivable. The following uses of Colorado resident DNA and genetic data are absolutely prohibited regardless of consent, contractual provision, or any other instrument:

(a) Use of genetic data in any insurance underwriting, premium calculation, coverage determination, or claims processing — this prohibition extends and supersedes the Genetic Information Nondiscrimination Act (GINA), 42 U.S.C. §2000ff et seq., in Colorado to cover all insurance lines, not just health and employment;

(b) Use of genetic data in any employment decision — hiring, promotion, termination, compensation, assignment, or any other term or condition of employment;

(c) Use of genetic data to train any AI model for any purpose other than the specific medical or research purpose for which consent was obtained;

(d) Transfer of genetic data to any law enforcement agency, foreign government, foreign entity, or intelligence agency absent a specific judicial warrant issued by a Colorado court of competent jurisdiction upon a showing of probable cause specific to the individual whose data is sought — familial DNA searching is prohibited absent individual warrants for each family member whose data would be accessed;

(e) Sale, license, or transfer of genetic data to any entity not covered by the original consent — including in any corporate transaction, asset sale, merger, or bankruptcy proceeding; and

(f) Retention of genetic data beyond the consent period or beyond the certified deletion date — the covered operator's obligation to delete is absolute and no business continuity interest overrides it.

(4) Familial genetic data extension. Because DNA discloses information about biological relatives:

(a) A Colorado resident's DNA data is treated as partially belonging to each of the resident's first-degree biological relatives — parents, siblings, children — for purposes of the prohibition on law enforcement access under subsection (3)(d); a warrant for one family member's genetic data does not authorize access to another family member's genetic data held by a covered operator;

(b) A covered operator that receives a law enforcement request for genetic data that would implicate first-degree relatives of the named subject shall notify the ODO within twenty-four (24) hours — the ODO shall assess whether the request constitutes indirect familial genetic surveillance and may challenge the request on the family members' behalf as a matter of public interest; and

(c) Ancestry service providers holding Colorado resident DNA data shall provide every Colorado resident in their database with a Familial Genetic Transparency Report annually — identifying all instances in which the resident's genetic data was used to identify, locate, or profile any biological relative, directly or through probabilistic matching.

(5) Genetic data bankruptcy immunity — absolute. Notwithstanding §15-15-166 and any other provision of law:

(a) Colorado resident DNA and genetic data is not property of the bankruptcy estate of any covered operator under any circumstances — it is not an asset that may be sold, transferred, licensed, or otherwise disposed of in any bankruptcy proceeding;

(b) Upon the filing of a bankruptcy petition by any covered operator holding Colorado resident genetic data, the ODO shall immediately seek an emergency injunction in Colorado state court prohibiting any transfer of Colorado resident genetic data pending resident election under §15-15-166(4);

(c) The only permitted disposition of Colorado resident genetic data in a covered operator bankruptcy is certified deletion — transfer to another operator is only permitted upon affirmative, specific, individual consent from each affected resident; and

(d) Any acquirer of a covered operator's assets in bankruptcy who receives Colorado resident genetic data without compliant individual consent is immediately subject to a Critical Severity Violation under Annex E and a civil penalty of ten thousand dollars ($10,000) per resident record received.

SECTION 24-20-171. QUANTUM INFRASTRUCTURE EMERGENCY FUNDING — IMMEDIATE AVAILABILITY — GENERAL FUND EMERGENCY LOAN — TRUST

INFRASTRUCTURE AS HIGHEST PRIORITY — REPAYMENT ARCHITECTURE — PROP 117 COMPLIANCE

24-20-171. Quantum Infrastructure Emergency Fund — immediate availability upon enactment — General Fund emergency loan authority — 9.9% of prior-year General Fund appropriations cap — Trust infrastructure as highest-priority state security investment — accelerated first-year deployment — automatic repayment from Enterprise Mitigation Revenue — Proposition 117 compliance — no voter approval required.

(1) Legislative findings and priority declaration. The general assembly finds and declares that:

(a) The quantum computing threat to current cryptographic infrastructure is not a future risk — it is a present and accelerating risk; adversarial nation-states are currently harvesting encrypted data under a 'harvest now, decrypt later' strategy, meaning that data encrypted today under current FIPS standards will be decryptable when quantum computing achieves sufficient scale — which NIST and the National Security Agency project to occur within this decade;

(b) The Colorado Trust of Unique and Identifying Information — holding the Digital Soul data, Master Deed registrations, Live Legal Mode session records, Police Encounter Protocol recordings, and financial data of every registered Colorado resident — is a high-value target for precisely this kind of adversarial data harvesting;

(c) Quantum-resistant cryptographic infrastructure for the Trust is not merely a technological upgrade — it is the foundational security guarantee that makes every other provision of this act meaningful; a Trust that can be decrypted by a quantum computer is a Trust that cannot be trusted;

(d) Waiting for Enterprise Mitigation Revenue to accumulate before funding quantum-resistant Trust infrastructure creates an unacceptable window of vulnerability — the Trust will begin holding resident data from the first day of operation, and that data must be quantum-resistant from the first day;

(e) The General Fund emergency loan mechanism established in this section is not an appropriation — it is a self-repaying loan secured by first-priority Enterprise Mitigation Revenue — the General Fund bears no net cost; and

(f) The general assembly declares that quantum-resistant Trust infrastructure is the highest-priority capital expenditure in this act — higher priority than any program, any distribution, any infrastructure investment, and any other use of Enterprise Mitigation Revenue — because without a secure Trust, no other provision of this act can be enforced.

(2) Quantum Infrastructure Emergency Fund — establishment and immediate availability. A Quantum Infrastructure Emergency Fund (QIEF) is established within the CCPAME operating structure, separate from the Colorado Automation Mitigation Trust, funded as follows:

(a) Immediate General Fund emergency loan — within sixty (60) days of this act's effective date, the State Treasurer shall transfer to the QIEF an amount equal to nine and nine-tenths percent (9.9%) of the prior fiscal year's total General Fund appropriations as an emergency infrastructure loan. The 9.9% cap is intentional and precise — it remains below the ten percent (10%) threshold that would trigger a revenue

increase vote requirement under Proposition 117 and C.R.S. §24-77-104. This is a loan, not an appropriation — it does not increase the Enterprise's revenue authority and does not trigger Proposition 117;

(b) The QIEF emergency loan is secured by a first-priority lien on all future Enterprise Mitigation Revenue — before resident distributions, before program accounts, before operating costs — until fully repaid;

(c) Repayment schedule: The QIEF emergency loan shall be repaid from Enterprise Mitigation Revenue at a rate of not less than twenty percent (20%) of monthly Enterprise Mitigation Revenue collections until the loan is fully repaid, with interest at the State's cost of funds. Projected full repayment within eighteen (18) months of first Enterprise Mitigation Revenue collection at base-case revenue scenario; and

(d) The State Treasurer shall report quarterly to the General Assembly on QIEF loan repayment status — the report shall show the outstanding balance, the repayment rate, and the projected full repayment date.

(3) Permitted uses — QIEF funds are restricted to quantum-resistant Trust infrastructure only. QIEF funds may be used exclusively for:

(a) Hardware security module (HSM) upgrades to FIPS 140-3 Level 4 — the highest available certification — for all Trust cryptographic operations;

(b) Implementation of NIST post-quantum cryptographic standards (FIPS 203 — ML-KEM, FIPS 204 — ML-DSA, FIPS 205 — SLH-DSA) and any subsequent NIST post-quantum standards published before full Trust deployment;

(c) Quantum key distribution (QKD) infrastructure for Trust node interconnects — providing information-theoretically secure key exchange that cannot be compromised by any computational attack, quantum or classical;

(d) Air-gapped backup Trust node construction with quantum-resistant cryptography — ensuring continuity of Trust operations under Systemic Continuity Protocol conditions;

(e) Independent third-party quantum security audit of the full Trust architecture before the Trust becomes operational — conducted by a NIST-certified laboratory, report published on the Public Accountability Dashboard; and

(f) Ongoing quantum threat monitoring — a real-time feed of NIST, NSA, and academic quantum computing development indicators integrated into the ODO's security operations center, with automatic escalation to the Cryptographic Standards Emergency Upgrade Authority under §10-10-305 when threat indicators cross defined thresholds.

(4) Deployment timeline — quantum security before first data collection. The QIEF-funded quantum-resistant infrastructure shall be fully operational before the Trust accepts its first resident registration. The ODO shall certify, in writing published on the Public Accountability Dashboard, that the Trust's quantum-resistant infrastructure meets NIST post-quantum standards before the Master Deed Registry opens for registration. No resident data shall be collected, stored, or processed in the Trust until this certification is published. This is the one provision of this act that cannot be phased — quantum security is a precondition of operation, not a phase-two upgrade.

(5) Proposition 117 compliance analysis — self-executing findings. The general assembly makes the following findings to support the Proposition 117 compliance of the QIEF emergency loan:

(a) The QIEF emergency loan is not 'enterprise revenue' under Proposition 117 — it is a loan from the General Fund to a state enterprise, repayable with interest from enterprise revenue; loans are not revenue;

(b) The 9.9% cap ensures that even if the QIEF loan were characterized as enterprise revenue, it would not trigger the ten percent (10%) threshold requiring voter approval under C.R.S. §24-77-104 — the cap is intentionally set at 9.9% with a margin of safety;

(c) The CCPAME is a state enterprise exempt from TABOR's spending limits to the extent of its enterprise revenues — the QIEF loan repayment from enterprise revenue is within the enterprise's TABOR-exempt operations; and

(d) The Attorney General shall, within thirty (30) days of this act's effective date, publish a formal opinion confirming the Proposition 117 compliance of the QIEF emergency loan structure — and shall, if requested by the CCPAME, defend that compliance in any legal challenge.

(6) No substitution — quantum funding is not available for other purposes. QIEF funds may not be redirected, swept, reprogrammed, or used for any purpose other than quantum-resistant Trust infrastructure under subsection (3). No executive order, legislative appropriation act, or CCPAME board vote may redirect QIEF funds. Any attempt to redirect QIEF funds is void ab initio and the State Treasurer shall reverse any such transfer within five (5) business days. The quantum infrastructure is the floor beneath which no other priority may descend.

PRIORITY PROVISIONS — SINGLE-SUBJECT NEXUS AND CONSTITUTIONAL BASIS

Section	Provision	Single-Subject Nexus	Why This Cannot Wait
§15-15-170 Voter Data Sovereignty	The State owns the tally. The voter owns the vote.	Voter registration and voting history data is Digital Soul processed by covered political data operators at industrial scale — the political data industry is one of the largest covered operator categories; regulation of its data extraction is squarely within single subject	Democracy depends on the secret ballot. The digital-era equivalent of the secret ballot is voter data sovereignty. The commercial political data industry profits from destroying it. Political Data Operations Premium 1.5x fee rate reflects the heightened democratic harm. AI-assisted voter targeting is a Class 5 felony.
§15-15-171 DNA Absolute Protection	DNA is the resident at the molecular level — non-waivable, permanent, familial extension	DNA data is Digital Soul at its most intimate — covered operators include 23andMe-model services, pharmaceutical AI platforms, and health tech companies; all are covered operators processing resident biological data	23andMe's 2025 bankruptcy demonstrated the catastrophic risk — a company holding 15 million people's DNA files for bankruptcy and the data goes to the auction block. Never in Colorado. DNA is not a bankruptcy asset. It is not an insurance underwriting tool. It is not a law enforcement fishing net. These prohibitions are absolute and permanent.

§24-20-171 Quantum Emergency Funding	9.9% General Fund loan — immediate — quantum-resistant Trust before first data collection — first-priority repayment lien	The Trust is the enforcement infrastructure for all Digital Soul property rights — without a quantum-secure Trust, the enforcement infrastructure is compromised; Trust security is the precondition of every other provision	Adversarial actors are harvesting data now to decrypt later. The Trust holds the most sensitive data in Colorado state history. It must be quantum-resistant on Day 1 — not Phase 2. The 9.9% General Fund loan is repaid within 18 months from first revenue. The General Fund bears no net cost. This is the one provision that cannot wait for revenue to accumulate.

The state owns the tally. The voter owns the vote. DNA is not a bankruptcy asset. Quantum security before first data collection.

AMPLIFY ACT v28 — FINAL ADDITIONAL IMPROVEMENTS

§§15-15-172 · 15-15-173 · 15-15-174 · 24-20-172 · 10-10-307

Annual Audit Right · Dark Pattern Prohibition · Child Online Safety · Public Franchise Receivership · AI Ethics Disclosure

---

SECTION 15-15-172. ANNUAL DIGITAL SOUL AUDIT RIGHT — COMPLETE OPERATOR ACCOUNTING — WHAT THEY HAVE, WHAT THEY DID, WHAT THEY EARNED, WHAT THEY OWE

15-15-172. Annual Digital Soul Audit Right — every registered Master Deed holder entitled to complete annual accounting from every covered operator processing their Digital Soul — data inventory, processing log, revenue attribution, fee obligation, deletion verification — plain-language format — CCPAME enforcement.

(1) Legislative finding. The general assembly finds that a property right without an accounting right is incomplete. A landowner can survey their land. A bank account holder can review their statement. A Colorado resident whose Digital Soul is being processed by covered operators generating Enterprise Mitigation Revenue has the right to a complete, plain-language annual accounting of exactly what those operators hold, what they did with it, what they earned from it, and what they owe in Enterprise Mitigation fees attributable to that resident's data. The Annual Digital Soul Audit Right is the accounting statement for the resident's most valuable property.

(2) Annual Digital Soul Audit — contents. Every covered operator processing a registered Master Deed holder's Digital Soul shall provide the resident with an Annual Digital Soul Audit within sixty (60) days of each calendar year-end, delivered to the resident's Resident Automated Mitigation Account dashboard, containing:

(a) Data Inventory — a complete enumeration of every category of the resident's Digital Soul held by the operator as of December 31, the volume of data in each category, the source of each category, and the date of first collection;

(b) Processing Log — a plain-language description of every processing activity performed on the resident's Digital Soul during the calendar year — training, inference, transfer, sale, license, anonymization, aggregation, and any other processing — with the business purpose stated for each;

(c) Revenue Attribution Statement — the operator's good-faith estimate of the Enterprise Mitigation Revenue attributable to the resident's Digital Soul during the calendar year, based on the resident's proportional contribution to the operator's total Colorado-nexus token output — presented as both a dollar figure and a percentage of the resident's total annual UFIPA Income Distribution and Resident Mitigation Dividend;

(d) Third-Party Disclosure Log — every entity to which any portion of the resident's Digital Soul was transferred, sold, licensed, or otherwise disclosed during the calendar year, the category of data transferred, the stated purpose, and the contractual basis;

(e) Active Consent Inventory — every Decentralized Identity Verification Protocol consent currently active for the resident, the scope of each consent, the date of execution, and the expiration or renewal date; and

(f) Deletion Verification — cryptographic proof of deletion for any resident Digital Soul data deleted during the calendar year, with the deletion date and the reason for deletion.

(3) Plain-language format requirement. The Annual Digital Soul Audit shall be presented in plain language accessible to a resident without legal or technical training — at a reading level not exceeding eighth grade for the summary section, with technical detail available in an appendix. The CCPAME shall publish a model Annual Digital Soul Audit template that covered operators may use for compliance. Audits that are incomprehensible, excessively technical, or deliberately obscure are a compliance failure subject to Tier 2 enforcement.

(4) Right to dispute. A resident who identifies an error, omission, or unauthorized processing in their Annual Digital Soul Audit may file a Dispute Notice with the CCPAME within ninety (90) days of receiving the Audit. The CCPAME shall investigate and issue a determination within sixty (60) days. If the dispute is substantiated, the covered operator is subject to Tier 2 statutory damages per record affected.

SECTION 15-15-173. DARK PATTERN PROHIBITION — DECEPTIVE UI DESIGN AGAINST RESIDENT DIGITAL SOUL INTERESTS — CONSENT MANIPULATION — STATUTORY DAMAGES — PER-SCREEN VIOLATION STANDARD

15-15-173. Dark pattern prohibition — deceptive user interface design manipulating resident Digital Soul consent — enumerated prohibited patterns — per-screen per-day violation standard — CCPAME pattern registry — private right of action — minors enhanced protection.

(1) Legislative finding. The general assembly finds that covered operators routinely deploy deceptive user interface design — dark patterns — specifically engineered to manipulate residents into consenting to broader Digital Soul data collection than the resident intends, or to make revocation of consent artificially difficult. Dark patterns are not neutral design

choices — they are engineered manipulation of the resident's property rights. Every dark pattern deployed against a Colorado resident's Digital Soul consent is a violation of the resident's inalienable property right, regardless of whether formal consent was technically obtained.

(2) Prohibited dark patterns. The following user interface design practices are prohibited when used in connection with any Digital Soul consent request, revocation process, or data access exercise:

(a) Confirmshaming — using emotionally manipulative or guilt-inducing language for the opt-out or revocation option, such as 'No thanks, I don't care about my privacy' or 'I prefer to share everything';

(b) Roach motel — making consent easy to give and artificially difficult to revoke — including requiring multiple steps, separate account screens, phone calls, mailed letters, or waiting periods for revocation that are not required for consent;

(c) Hidden defaults — pre-selecting consent to the broadest data collection option and requiring affirmative action to select a more restrictive option, when the Decentralized Identity Verification Protocol requires affirmative consent;

(d) Interface interference — visually obscuring, minimizing, graying out, or making difficult to locate the revocation option or the option to limit data collection relative to the option to consent to broad collection;

(e) Misdirection — drawing visual attention away from material data collection disclosures through animation, color, placement, or size differential that causes a reasonable user to miss key information;

(f) Disguised ads — presenting sponsored content, data collection requests, or consent solicitations in a format designed to appear as neutral system messages, notifications, or required steps;

(g) Forced continuity — conditioning continued service access on consent to data collection beyond what is required for the service, when an alternative without the required consent exists; and

(h) Trick questions — using confusing double negatives, misleading phrasing, or ambiguous language in consent requests such that a reasonable resident cannot determine what they are consenting to.

(3) Violation standard and damages. Each prohibited dark pattern deployed on a unique screen or interface element is a separate violation. Damages: five hundred dollars ($500) per unique screen per day the dark pattern is deployed. A covered operator who deploys the same dark pattern across multiple screens of an application is liable for $500 per screen per day. CCPAME may assess penalties administratively upon pattern detection through the Open API monitoring system. Residents may file private actions directly.

(4) Enhanced protection for minors. Any dark pattern deployed against a user interface accessible to minors — including any platform, application, or service with more than five percent (5%) minor users — is subject to triple damages: one thousand five hundred dollars ($1,500) per screen per day. The operator's knowledge of minor users is presumed if the platform is directed at minors or if the operator has age-related analytics indicating minor usage.

(5) CCPAME Dark Pattern Registry. The CCPAME shall maintain a publicly accessible Dark Pattern Registry on the Public Accountability Dashboard, listing all covered operators with active or resolved dark pattern violations, the pattern type, the remediation status, and the damages assessed. The Registry is searchable by operator name and pattern type.

Researchers, journalists, and residents may submit pattern reports to the ODO for investigation.

SECTION 15-15-174. CHILD ONLINE SAFETY EXTENSION — UNDER-13 ABSOLUTE PROHIBITION — PARENTAL MASTER DEED AUTHORITY — AGE-APPROPRIATE DESIGN MANDATE — SCHOOL PLATFORM RESTRICTIONS

15-15-174. Child online safety extension — under-13 absolute Digital Soul processing prohibition — parental Master Deed registration authority — age-appropriate design code — school and educational platform restrictions — algorithmic amplification prohibition for minors — enhanced damages.

(1) Legislative finding. The general assembly finds that: (a) Children under the age of thirteen (13) cannot meaningfully consent to Digital Soul data processing — their cognitive development does not support informed, voluntary, and specific consent to complex data processing regimes; (b) The commercial incentive to collect data from children is enormous — children are lifelong data subjects and their behavioral data has significant predictive value for commercial purposes; (c) Children in school settings are particularly vulnerable — educational technology platforms process vast quantities of student behavioral, academic, and social data, often without meaningful parental knowledge or consent; and (d) Algorithmic amplification systems — recommendation engines, engagement maximization algorithms, and behavioral reinforcement loops — pose documented harm to minor mental health and are among the most powerful applications of covered automation activity.

(2) Under-13 absolute prohibition. No covered operator may collect, process, store, transfer, or use the Digital Soul of any Colorado resident under the age of thirteen (13) for any commercial purpose. The prohibition is absolute — no parental consent, no terms of service provision, and no business necessity argument overrides it. Under-13 Digital Soul is categorically beyond the reach of covered operator commercial processing. Permitted processing is limited to: (a) minimum necessary technical operations required to deliver a service specifically requested by a parent or guardian; (b) safety and security operations required to protect the child from imminent harm; and (c) legally mandated reporting under child welfare statutes.

(3) Parental Master Deed registration authority. A parent or legal guardian of a Colorado resident minor between the ages of thirteen (13) and seventeen (17) inclusive may: (a) Register a Master Deed on behalf of the minor; (b) Review the minor's Annual Digital Soul Audit; (c) Exercise the Universal Telemetry Allowance on the minor's behalf; (d) Revoke any Decentralized Identity Verification Protocol consent on the minor's behalf with immediate effect; and (e) Activate Live Legal Mode on the minor's behalf for any violation of the minor's Digital Soul rights. At age fourteen (14), the minor gains co-equal access alongside the parent. At majority, the minor assumes full independent authority and parental access is automatically revoked.

(4) Age-appropriate design mandate. Any covered operator whose platform, application, or service is used by Colorado residents under the age of eighteen (18) — including any service where minor users exceed five percent (5%) of the Colorado user base — shall: (a) Default to the highest available privacy setting for any user whose age is unknown or unverified; (b) Prohibit behavioral advertising targeting based on Digital Soul data for any user under eighteen (18); (c) Disable engagement maximization algorithms — including infinite scroll, autoplay, push notification optimization, and variable reward scheduling — for verified minor users; and (d) Provide parents with a real-time Minor Activity Dashboard accessible through the myColorado platform showing the categories of data collected from the minor and all processing activities.

(5) School and educational platform restrictions. Any covered operator providing services under contract to a Colorado school district, charter school, or educational institution: (a) May process student Digital Soul data only for the specific educational purpose specified in the contract — no secondary commercial use, no advertising, no model training on student data beyond the contracted educational service; (b) May not transfer student Digital Soul data to any third party for any purpose without written consent from the student's parent or guardian for each specific transfer; (c) Must delete all student Digital Soul data within thirty (30) days of the student's enrollment ending — no retention for alumni targeting, product development, or any other purpose; and (d) Is subject to a Educational Platform Premium of 2.0x on all base Enterprise Mitigation fee rates, reflecting the heightened vulnerability of the student population and the school's position of trust.

(6) Algorithmic amplification prohibition. No covered operator may deploy an algorithmic amplification system — recommendation engine, engagement maximization algorithm, or behavioral reinforcement loop — that uses a Colorado minor's Digital Soul to predict and maximize engagement in a manner that: (a) Prioritizes emotionally activating, distressing, or conflict-generating content; (b) Creates filter bubbles isolating the minor from diverse viewpoints; or (c) Detects and exploits psychological vulnerability signals in the minor's behavioral data to increase time-on-platform. Violation is a Critical Severity offense — the covered operator's entire Colorado platform is suspended pending remediation, not just the algorithm affecting the minor.

SECTION 24-20-172. PUBLIC FRANCHISE RECEIVERSHIP PROTOCOL — OPERATOR LOYALTY FAILURE — COURT-SUPERVISED RECEIVERSHIP — FRANCHISE CONTINUITY — OPERATOR FINANCIAL INTEREST PRESERVED — NEW FRANCHISEE CERTIFICATION

24-20-172. Public Franchise Receivership Protocol — trigger conditions — CCPAME petition for court-supervised receivership — receiver duties — Public Franchise Asset operational continuity — operator financial interest preserved during receivership — new franchisee certification — graduation from receivership.

(1) Legislative finding. The general assembly finds that the Colorado Emergent Capability Public Franchise Protocol is designed to be a promotion, not a punishment — enrollment as a Public Franchise Asset signals that a covered automation system has demonstrated capabilities significant enough to warrant protection as essential public infrastructure. The Public Franchise Receivership Protocol completes this framework: just as a public utility whose operator abandons its service territory enters receivership to ensure service continuity — not to destroy the operator's financial interest — a Public Franchise Asset whose operator fails their Operator Loyalty Obligation enters receivership to ensure continuity of the public benefit while preserving the operator's economic stake pending a new franchisee certification.

(2) Receivership trigger conditions. The CCPAME shall petition the Denver District Court for appointment of a Public Franchise Receiver upon: (a) An operator's material breach of the Operator Loyalty Obligation under §10-10-303(6) — including directing the Public Franchise Asset to operate against its registered owner's interests, disclosing resident data without authorization, or accepting government direction contrary to resident interests; (b) An operator's abandonment of the Public Franchise Charter obligations — including failure to provide public benefit services, failure to pay enhanced Enterprise Mitigation fees for sixty (60) or more days, or voluntary exit from the Colorado market; (c) An operator's insolvency under §15-15-166 where the Public Franchise Asset is material to the operator's operations; or (d) An operator's foreign acquisition under §15-15-166(6) where the CCPAME determines the acquisition presents unacceptable security risk.

(3) Receiver appointment and duties. The court shall appoint a Public Franchise Receiver — a qualified technology operations professional from a CCPAME-certified panel — within fourteen (14) days of the CCPAME's petition. The Receiver shall: (a) Take operational custody of the Public Franchise Asset and all systems necessary for its continued operation; (b) Continue all Public Franchise Charter public benefit obligations without interruption; (c) Maintain all resident Digital Soul protections and Operator Loyalty Obligations as if the Receiver were the original operator; (d) Preserve and report on the operator's financial interest in the Public Franchise Asset — the Receiver does not extinguish the operator's economic stake; (e) Publish quarterly Receivership Status Reports on the Public Accountability Dashboard; and (f) Seek a new certified franchisee within one hundred eighty (180) days of appointment.

(4) Operator financial interest preservation. The operator's financial interest in the Public Franchise Asset — its equity stake, intellectual property rights, and economic value — is preserved through receivership. The Receiver manages operations for the public benefit; the operator retains the economic upside of the asset's continued operation. Enhanced Enterprise Mitigation fees continue to accrue and are paid first to the CCPAME; remaining revenue is held in trust for the operator pending receivership resolution. The operator does not lose its investment — it loses its management authority until a compliant new franchisee is certified or the operator cures its breach and resumes franchise obligations.

(5) New franchisee certification. The CCPAME shall establish a Public Franchise Certification process for entities seeking to assume franchise obligations for a Public Franchise Asset in receivership. Certification requires: (a) Demonstrated technical capacity to operate the Public Franchise Asset; (b) Financial capacity to meet Public Franchise Charter obligations; (c) CCPAME board approval by a four-fifths (4/5) vote; (d) Public hearing with not fewer than thirty (30) days notice; and (e) Execution of a new Public Franchise Charter with updated public benefit obligations appropriate to the Asset's current capabilities. Upon new franchisee certification, receivership terminates and operational custody transfers to the new franchisee.

(6) Graduation — voluntary franchise enhancement. An operator of a Public Franchise Asset that consistently exceeds its Public Franchise Charter obligations — maintaining full Operator Loyalty compliance, expanding public benefit services, and achieving a five-year record of enhanced Enterprise Mitigation fee contribution above 110% of the Charter's required level — may petition the CCPAME for Public Franchise Graduation status. Graduation status: (a) Reduces the enhanced fee rate multiplier from 2.0x to 1.75x; (b) Converts the Public Franchise Charter from a CCPAME-administered document to a jointly negotiated instrument; and (c) Entitles the operator to a Public Franchise Seal — a publicly displayed certification that the operator is a compliant Public Franchise Asset operator serving Colorado's public benefit. Graduation creates the incentive for operators to view franchise enrollment as a privilege worth maintaining, not a burden to escape.

SECTION 10-10-307. COVERED OPERATOR AI ETHICS DISCLOSURE — TRAINING DATA PROVENANCE — OBJECTIVE FUNCTION DISCLOSURE — FUNDING SOURCE TRANSPARENCY — BIAS AUDIT REQUIREMENT — PUBLIC ACCOUNTABILITY DASHBOARD INTEGRATION

10-10-307. Covered operator AI ethics disclosure — annual training data provenance report — objective function and optimization target disclosure — funding source transparency — third-party bias audit — results published on Public Accountability Dashboard — residents entitled to know what the AI was built to do and who paid for it.

(1) Legislative finding. The general assembly finds that: (a) A resident interacting with a covered operator's AI system has a right to know what that system was designed to optimize — an AI designed to maximize engagement has fundamentally different interests than an AI designed to provide accurate information, and the resident deserves to know which they are dealing with; (b) The funding source of an AI system shapes its objective function — an AI funded by advertising revenue is optimized for attention capture; an AI funded by insurance companies may be optimized to deny claims; a resident whose Digital Soul is processed by these systems has a right to know who built them and why; (c) AI systems trained on biased data produce biased outputs that can harm residents in consequential decisions — employment, credit, housing, healthcare — and covered operators must be accountable for the bias profile of their systems; and (d) These disclosures cost covered operators nothing in operational terms — they require transparency about design choices already made, not changes to those choices.

(2) Annual AI Ethics Disclosure — required contents. Every covered operator shall publish an Annual AI Ethics Disclosure within ninety (90) days of each calendar year-end, submitted to the CCPAME and published on the Public Accountability Dashboard. The Disclosure shall contain:

(a) Training Data Provenance Report — identification of the major categories of data used to train the operator's covered automation systems, the geographic sources of that

data, whether Colorado resident data was included and in what volume, and whether training data was obtained through consent-based or non-consent-based collection;

(b) Objective Function Disclosure — a plain-language statement of the primary optimization target of each covered automation system — what the system is designed to maximize, minimize, or achieve — and who defined that objective function and when;

(c) Funding Source Transparency — identification of the primary commercial revenue sources that fund the development and operation of each covered automation system — advertising revenue, subscription revenue, enterprise contracts, government contracts, or other sources — and the proportion of revenue from each source;

(d) Consequential Decision Inventory — identification of every category of consequential decision affecting Colorado residents in which the operator's covered automation systems play a material role — including employment screening, credit scoring, housing applications, healthcare triage, insurance underwriting, criminal justice risk assessment, and content moderation; and

(e) Third-Party Bias Audit Results — for any covered automation system used in consequential decisions affecting Colorado residents, the results of an independent third-party bias audit conducted within the prior two (2) years, including the audit methodology, the demographic categories analyzed, the disparity ratios found, and the remediation steps taken. Covered operators that cannot demonstrate a bias audit within two years are subject to a Bias Audit Surcharge of 0.5x on their base Enterprise Mitigation fee rates until a compliant audit is completed and submitted.

(3) Plain-language summary requirement. The Annual AI Ethics Disclosure shall include a one-page plain-language summary accessible to residents without technical training. The summary shall answer three questions in plain English: What does this AI try to do? Who paid for it? Has it been checked for fairness? The CCPAME shall publish model language and a model summary template.

(4) Public Accountability Dashboard integration. All Annual AI Ethics Disclosures are published on the CCPAME Open API and accessible through the Public Accountability Dashboard. Residents searching for a covered operator can view that operator's complete ethics disclosure history. The Dashboard shall flag: (I) operators who have not filed a current Disclosure; (II) operators with unresolved bias audit findings; and (III) operators whose objective function disclosure reveals a direct conflict with resident interests — such as engagement maximization systems used on minors.

ADDITIONAL IMPROVEMENTS — SINGLE-SUBJECT NEXUS AND SYSTEM IMPACT

Section	What	Why It Fits Single Subject	System Impact
§15-15-172 Annual Audit Right	Complete annual accounting — data held, processing done, revenue attributed, third parties, active consents, deletion proof	A property right without an accounting right is incomplete — the audit is the property statement for Digital Soul	Residents know exactly what operators have and what it earned. Revenue Attribution Statement shows residents their proportional contribution to the distributions they

			receive. Closes the information asymmetry permanently.
§15-15-173 Dark Pattern Prohibition	$500/screen/day per prohibited UI manipulation pattern — $1,500/screen/day for minors — CCPAME Dark Pattern Registry — private right of action	Consent manipulation undermines the Decentralized Identity Verification Protocol — dark patterns are an attack on the Digital Soul property right's consent foundation	Every consent-manipulation technique that currently generates billions in unauthorized data collection becomes $500/screen/day. The business model of dark-pattern consent extraction collapses.
§15-15-174 Child Online Safety	Under-13 absolute prohibition — parental Master Deed authority — age-appropriate design mandate — school platform 2.0x fee premium — algorithmic amplification prohibition — platform suspension for minor violations	Minor Digital Soul is the most vulnerable category — protections for minors are necessarily and properly connected to the Digital Soul property right framework	Under-13 data collection ends categorically. School platforms pay double. Engagement maximization algorithms targeting minors trigger full platform suspension. Parents get real-time dashboards. The most exploited population gets the strongest protection.
§24-20-172 Public Franchise Receivership	Complete the franchise architecture — court-supervised receiver on operator loyalty failure — operator financial interest preserved — new franchisee certification — graduation pathway reducing fee multiplier to 1.75x	Completes the Colorado Emergent Capability Public Franchise Protocol — receivership is the well-understood Colorado legal mechanism for utility service continuity when an operator fails	Operators now have a graduation incentive — five years of compliance above 110% of Charter requirements earns a fee reduction and a Public Franchise Seal. Enrollment is a privilege worth maintaining. Receivership is the backstop that makes the franchise permanent.
§10-10-307 AI Ethics Disclosure	Annual training data provenance, objective function, funding source, consequential decision inventory, bias audit — 0.5x surcharge for missing bias audit — Dashboard integration	Covered operator AI systems are the instruments through which Digital Soul data is processed — transparency about what those instruments are built to do is enforcement infrastructure for the property right	Residents know what the AI was built to optimize and who funded it. Consequential decision inventory identifies every AI affecting employment, credit, housing, healthcare. Bias audit requirement with fee surcharge creates financial incentive for fairness. The information asymmetry that enables manipulation is eliminated.

The state owns the tally. The voter owns the vote. DNA is not a bankruptcy asset. Quantum security before first data. The AI tells you what it was built to do. Dark patterns are $500 a screen a day. Under-13 is absolute. Public Franchise enrollment is a promotion.

AMPLIFY ACT v28 — BILL 1 FINAL COMPLETION SECTIONS

§§15-15-175 through 15-15-182

Biometric Data · Right to Explanation · Right to Correction · Employee Digital Soul · Whistleblower · Agricultural Digital Soul · Senior Protection · Reproductive Health · Incapacitated Adult · Data Minimization

---

SECTION 15-15-175. BIOMETRIC DATA PROTECTION — COLORADO BIOMETRIC PROPERTY ACT — CBPA —

PRIVATE RIGHT OF ACTION — $1,000–$5,000 PER VIOLATION

15-15-175. Biometric data as Digital Soul Protection Tier 1 — informed written consent before collection — retention schedule and destruction policy — no sale or profit from biometric data — private right of action $1,000 negligent / $5,000 intentional per violation — 5-year SOL — employer biometric prohibition.

(1) Legislative finding. The general assembly finds that biometric data — facial geometry, fingerprints, voiceprints, iris scans, retina scans, hand geometry, gait signatures, and any other measurement of the human body that uniquely identifies a person — is the most commercially exploited and least legally protected category of Digital Soul data in Colorado. Unlike a password or account number, biometric data cannot be changed if compromised. Illinois BIPA has generated over $1.5 billion in corporate accountability through private litigation in eight years — Colorado's CBPA adopts and strengthens that framework.

(2) Biometric data — defined categories. 'Biometric data' means: (a) a retina or iris scan; (b) a fingerprint or voiceprint; (c) a scan of hand or face geometry; (d) gait analysis data; (e) a vein pattern; (f) any other identifier based on an individual's unique biological characteristics that can be used to identify that specific individual. Biometric data does not include photographs, video recordings used solely for security purposes without facial recognition processing, or written signatures.

(3) Mandatory pre-collection requirements. Before collecting any biometric data from a Colorado resident, a covered operator shall: (a) inform the resident in writing that biometric data is being collected and the specific category of biometric data; (b) inform the resident in writing of the specific purpose and length of time for which the biometric data is being collected, stored, and used; (c) receive a written release executed by the resident — a general terms-of-service consent is insufficient; a biometric-specific, affirmative, dated, signed release is required; and (d) publish a publicly available written policy establishing a retention schedule and guidelines for permanently destroying biometric data when the initial purpose has been satisfied or within three (3) years of collection, whichever is earlier.

(4) Absolute prohibitions. No covered operator may: (a) sell, lease, trade, or otherwise profit from a resident's biometric data; (b) disclose or disseminate biometric data to any person other than: (I) the resident; (II) persons with written consent of the resident; (III) as required by state or federal law; or (IV) as required by valid warrant meeting the requirements of §10-10-303(5); (c) use biometric data for any purpose other than the specific purpose for which written release was obtained; or (d) use biometric data in any consequential decision — employment, credit, housing, insurance, law enforcement — without specific additional written consent for the consequential use.

(5) Private right of action — Colorado Biometric Property Act. Any resident aggrieved by a violation of this section may bring an action in Colorado courts and is entitled to recover for each violation: (a) actual damages or liquidated damages of one thousand dollars ($1,000) — whichever is greater — for each negligent violation; (b) actual damages or liquidated damages of five thousand dollars ($5,000) — whichever is greater — for each intentional or reckless violation; (c) reasonable attorney fees and costs; and (d) injunctive or other equitable relief. Violations by covered operators deploying biometric data collection at scale — defined as collection from more than one thousand (1,000) residents within any twelve-month period — are subject to a class action multiplier of three (3x) applied to liquidated damages.

(6) Statute of limitations. An action under this section must be brought within five (5) years of: (a) the date of the biometric data collection; or (b) the date the resident discovered or reasonably should have discovered the violation through the Annual Digital Soul Audit under §15-15-172 — whichever is later.

SECTION 15-15-176. RIGHT TO EXPLANATION — ALGORITHMIC DECISION TRANSPARENCY — RIGHT TO CORRECTION — INACCURATE DIGITAL SOUL REMEDY — $500/RECORD/DAY

15-15-176. Right to explanation — plain-language disclosure of algorithmic decision factors — consequential decisions defined — 30-day response obligation — right to correction — inaccurate Digital Soul correction request — 30-day correction window — $500/record/day for uncorrected inaccuracies — human review right.

(1) Right to Explanation. Any covered operator whose covered automation system makes or materially contributes to a consequential decision affecting a Colorado resident shall, upon the resident's written request submitted within ninety (90) days of the decision, provide a plain-language Explanation Notice within thirty (30) days containing: (a) the primary factors that determined the decision outcome; (b) the relative weight assigned to each factor; (c) the specific threshold or criteria the resident failed to meet; (d) the data sources used in making the determination, including any resident Digital Soul data categories; and (e) whether a human reviewed the decision and at what stage. 'Consequential decision' means any automated determination affecting employment, credit, housing, insurance, healthcare access, educational opportunity, government benefits, or law enforcement risk classification.

(2) Human review right. A resident who receives a negative consequential decision from a covered automation system has the right to request human review of that decision within thirty (30) days of receiving the Explanation Notice. The covered operator shall assign a qualified human reviewer — not an AI system reviewing AI output — who conducts an independent review and provides a written determination within forty-five (45) days. The human reviewer's determination supersedes the automated determination if the human reviewer finds material error.

(3) Right to Correction. A resident who identifies inaccurate Digital Soul data — whether through the Annual Digital Soul Audit under §15-15-172, the Explanation Notice under subsection (1), or any other means — may file a Correction Request with the covered operator within ninety (90) days of discovery. The Correction Request shall identify the specific inaccurate data and the basis for the claim of inaccuracy.

(4) Covered operator correction obligation. Upon receiving a Correction Request: (a) The covered operator shall investigate and either correct the inaccurate data or provide a written explanation of why the data is accurate within thirty (30) days; (b) If correction is made, the covered operator shall notify all third parties to whom the inaccurate data was transferred within the prior two (2) years and provide corrected data; (c) If correction is disputed, the

resident may file a complaint with the CCPAME for adjudication — CCPAME shall issue a determination within sixty (60) days; and (d) If inaccurate data is not corrected within thirty (30) days of a substantiated Correction Request, the covered operator is liable for five hundred dollars ($500) per record per day until correction is made — payable directly to the resident's Resident Automated Mitigation Account.

SECTION 15-15-177. EMPLOYEE DIGITAL SOUL PROTECTION — EMPLOYMENT MONITORING CONSENT REQUIREMENT — PROHIBITED ASSIGNMENTS — WHISTLEBLOWER PROTECTION — $25,000 RETALIATION DAMAGES

15-15-177. Employee Digital Soul — covered operator employment monitoring requires DID consent — prohibited waiver as employment condition — prohibited assignment — workplace surveillance limits — employee whistleblower protection — $25,000 retaliation damages — reinstatement.

(1) Employee Digital Soul protection. An employer that uses a covered automation system to monitor employee communications, productivity, keystrokes, location, behavioral patterns, biometrics, or any other employee Digital Soul is a covered operator processing that employee's Digital Soul. The employer-employee relationship does not diminish or modify the employee's Digital Soul property rights. All provisions of this act apply to employer processing of employee Digital Soul.

(2) Prohibited employment conditions. No employer may: (a) require an employee or job applicant to waive any Digital Soul right as a condition of employment, continued employment, promotion, or any employment benefit; (b) require an employee to consent to covered automation monitoring beyond what is reasonably necessary for the specific job function — general workplace surveillance consent is not valid DID consent for all monitoring purposes; (c) use covered automation monitoring to surveil employee union organizing activity, political activity, or any other activity protected under Colorado or federal law; or (d) process employee biometric data under §15-15-175 without complying with all requirements of §15-15-175 in addition to standard DID consent.

(3) Permitted workplace monitoring. An employer may use covered automation systems for: (a) monitoring directly work-product-related activity on employer-owned devices during work hours, with advance written notice to the employee; (b) physical security monitoring in designated areas with posted notice; and (c) safety monitoring required by federal or state occupational safety law. Monitoring permitted under this subsection still requires DID consent — the scope of consent is limited to the permitted monitoring purpose.

(4) Employee Digital Soul whistleblower protection. A Colorado employee who in good faith reports to the CCPAME, ODO, Colorado Attorney General, or any law enforcement agency a covered operator violation of this act — including the employee's own employer — is protected from: (a) termination; (b) demotion; (c) suspension; (d) harassment or hostile work environment; (e) reduction in pay or hours; or (f) any other adverse employment action.

Retaliation against a whistleblower employee is: (I) a Critical Severity Violation; (II) subject to statutory damages of twenty-five thousand dollars ($25,000) per incident; (III) subject to mandatory reinstatement with back pay; and (IV) grounds for immediate covered operator registration suspension pending remediation.

(5) Qui tam — employee whistleblower bounty. An employee whose whistleblower report results in a CCPAME enforcement action collecting statutory damages is entitled to twenty percent (20%) of the damages collected — paid from the enforcement recovery before the remainder flows to the affected residents' accounts. No employer may contractually prohibit employees from making whistleblower reports or receiving whistleblower bounties. Any such prohibition is void as against public policy.

SECTION 15-15-178. AGRICULTURAL DIGITAL SOUL — FARM DATA AS DIGITAL SOUL — FARMER DATA COOPERATIVE — PRECISION AGRICULTURE OPERATOR OBLIGATIONS — RURAL COLORADO CONSTITUENCY

15-15-178. Agricultural Digital Soul defined — farm operational data, soil data, yield data, crop genetics, equipment telemetry as Digital Soul — precision agriculture covered operators — Farmer Data Cooperative formation — same property right framework — Rural Digital Soul Dividend — CCPAME rural outreach mandate.

(1) Legislative finding. The general assembly finds that Colorado's 36,000 farms generate vast quantities of commercially valuable data through precision agriculture platforms — soil composition, yield maps, crop genetics, equipment telemetry, agronomic decisions, and weather correlation data. Precision agriculture operators including equipment manufacturers, seed companies, insurance actuaries, commodity traders, and agrochemical companies extract enormous commercial value from this farm data without meaningful farmer consent or compensation. Agricultural Digital Soul is the farmer's most valuable property after the land itself.

(2) Agricultural Digital Soul defined. 'Agricultural Digital Soul' means all data generated by or derived from a Colorado agricultural operation, including: (a) soil composition, fertility, and microbiome data; (b) crop yield, quality, and variety performance data; (c) precision agriculture equipment telemetry — planting, spraying, harvesting, and tillage data; (d) irrigation consumption and efficiency data; (e) livestock behavioral, health, and production data; (f) farm financial and operational decision data processed through covered automation systems; (g) agronomic recommendation data generated by AI advisory systems; and (h) any data enabling identification, profiling, or competitive analysis of a specific agricultural operation or operator. Agricultural Digital Soul is the inalienable intangible personal property of the farm operator at Protection Tier 2 under this act.

(3) Precision agriculture covered operators. Any covered automation system that collects, processes, or derives commercial value from Colorado Agricultural Digital Soul is a covered operator subject to all provisions of this act. Precision agriculture covered operators include but are not limited to: equipment manufacturers operating connected agricultural machinery

in Colorado; seed companies processing yield and variety performance data; crop insurance platforms using farm data for actuarial modeling; commodity trading platforms using farm production data; and agrochemical companies processing application and effectiveness data.

(4) Farmer Data Cooperative formation. Colorado farm operators who have registered Agricultural Digital Soul Master Deeds may form Farmer Data Cooperatives under C.R.S. §7-56-101 et seq. — with identical structure and CCPAME oversight as Resident Data Cooperatives under §24-20-159 — for collective negotiation of Premium Royalty rates with precision agriculture covered operators. A certified Farmer Data Cooperative representing not fewer than five hundred (500) registered Agricultural Digital Soul Master Deed holders may compel collective negotiation with any precision agriculture covered operator generating more than ten billion (10,000,000,000) tokens annually from Colorado Agricultural Digital Soul.

(5) Rural Digital Soul Dividend. The CCPAME shall establish a Rural Digital Soul Dividend as a subprogram of the Resident Mitigation Dividend, distributing not less than eight percent (8%) of annual Enterprise Mitigation Revenue attributable to precision agriculture covered operators directly to registered Agricultural Digital Soul Master Deed holders — calculated per registered farm acre, ensuring that larger operations receive proportionally higher distributions reflecting their proportionally larger Agricultural Digital Soul contribution.

(6) CCPAME rural outreach mandate. The CCPAME shall: (a) establish a Rural Digital Rights Office within twelve (12) months of enactment with not fewer than three staff members dedicated to Agricultural Digital Soul registration, compliance, and enforcement; (b) conduct not fewer than twenty-four (24) annual outreach events in Colorado agricultural communities; (c) partner with Colorado State University Extension to provide Agricultural Digital Soul registration assistance; and (d) publish all CCPAME materials in plain English and Spanish without technical jargon, with specific agricultural terminology guidance.

SECTION 15-15-179. SENIOR AND ELDER DIGITAL SOUL ENHANCED PROTECTION — AGE 65+ DEFAULT RESTRICTIONS — FINANCIAL EXPLOITATION PROHIBITION — ELDER ALAM MODULE — AARP PARTNERSHIP

15-15-179. Senior and elder Digital Soul enhanced protection — residents age 65+ default maximum privacy — financial product targeting prohibition — elder exploitation detection in ALAM — prohibited elder-targeted practices — CCPAME Elder Digital Rights Office — AARP and senior advocacy partnership.

(1) Legislative finding. The general assembly finds that Colorado residents age 65 and older are subject to documented and disproportionate commercial exploitation of their Digital Soul — their health data commands premium prices from pharmaceutical companies, their financial data is targeted by predatory financial products, their behavioral data enables manipulation of fixed-income populations with limited ability to recover from financial harm, and their unfamiliarity with digital consent mechanisms makes dark-pattern exploitation

especially effective. Colorado's 900,000+ residents over 65 constitute the state's highest-turnout voting demographic and are entitled to the strongest available Digital Soul protections.

(2) Age 65+ default to maximum privacy. Any covered operator that can determine or reasonably infer from Digital Soul data that a Colorado resident is age 65 or older shall: (a) default to the most restrictive available privacy setting for that resident without any action required by the resident; (b) require affirmative opt-in rather than opt-out for any data processing beyond the minimum necessary for the service requested; (c) prohibit any dark pattern under §15-15-173 in any interface used by the resident; and (d) provide all consent requests and privacy notices in font size not less than 14 points in plain English at a reading level not exceeding sixth grade.

(3) Elder financial exploitation prohibition. No covered operator may: (a) use an elder resident's Digital Soul to target financial products with annual interest rates exceeding thirty-six percent (36%); (b) use an elder resident's health data to target insurance products or supplements without specific affirmative written consent; (c) use behavioral data showing cognitive decline indicators — increased confusion signals, repetitive action patterns, unusual financial behavior — to increase commercial targeting; or (d) transfer elder resident financial behavior data to any entity not directly providing a service requested by the resident.

(4) Elder Digital Soul ALAM module. The ALAM under §10-10-302 shall include an Elder Digital Soul Module — activated automatically for residents who indicate age 65+ in their Master Deed registration — that runs enhanced background detection for: (a) elder financial exploitation patterns including predatory loan targeting, insurance fraud, and investment scheme indicators; (b) Medicare and Medicaid fraud indicators in billing and claims data; (c) Social Security and pension payment discrepancies; and (d) covered operator contract terms that violate elder consumer protection standards under C.R.S. §6-1-105. Detected violations generate automatic ALAM notifications and optionally initiate assisted Live Legal Mode sessions.

SECTION 15-15-180. REPRODUCTIVE HEALTH DATA ABSOLUTE PROTECTION — TIER 1 PROTECTION — OUT-OF-STATE LAW ENFORCEMENT PROHIBITION — CLINIC VISIT DATA — PREGNANCY STATUS — CONTRACEPTION DATA

15-15-180. Reproductive health data as Digital Soul Protection Tier 1 — absolute prohibition on law enforcement transfer without individual warrant — out-of-state proceeding prohibition — clinic visit location data — fertility and pregnancy data — contraception data — AI inference prohibition — Colorado constitutional right foundation.

(1) Legislative finding. The general assembly finds that post-Dobbs, location data showing visits to reproductive health clinics, search data showing reproductive health queries,

purchase data showing contraceptive acquisition, and health data showing pregnancy status, fertility treatment, or contraceptive use are being actively weaponized by law enforcement in states with abortion restrictions and purchased by anti-reproductive-rights advocacy organizations. Colorado is a reproductive rights protection state under the Colorado Reproductive Health Equity Act, C.R.S. §25-6-402, and the Digital Soul framework must protect the data infrastructure of that constitutional right with the same absoluteness.

(2) Reproductive health data — Protection Tier 1. 'Reproductive health data' means any data from which the following can be determined, inferred, or estimated: (a) pregnancy status, history, or outcome; (b) fertility treatment or assisted reproduction; (c) contraceptive use, prescription, or purchase; (d) visits to any reproductive health clinic, family planning facility, or abortion provider; (e) searches, queries, or communications related to reproductive health decisions; (f) purchase of pregnancy tests, contraceptives, or reproductive health products; or (g) any other data enabling inference about a resident's reproductive health status or decisions. Reproductive health data is Digital Soul at Protection Tier 1 — subject to all Tier 1 protections including annual affirmative consent renewal and absolute prohibition on covered operator processing for commercial purposes beyond the direct health service consented to.

(3) Absolute prohibitions — non-waivable. No covered operator may: (a) transfer reproductive health data to any law enforcement agency — Colorado or out-of-state — without an individual warrant issued by a Colorado court; a warrant from any out-of-state court or federal court does not authorize transfer of Colorado resident reproductive health data held by a Colorado-registered covered operator; (b) transfer reproductive health data to any entity in any state where that data could be used as evidence in a criminal proceeding related to reproductive health decisions; (c) use covered automation systems to infer reproductive health status from non-reproductive data — purchase patterns, location patterns, or search patterns — and apply that inference to any commercial or law enforcement purpose; (d) retain reproductive health data beyond the specific service transaction that generated it without annual affirmative renewal of specific consent; or (e) sell, license, or transfer reproductive health data to any anti-reproductive-rights advocacy organization, political organization, or data broker under any circumstances.

(4) Covered operator reporting — out-of-state demands. A covered operator that receives a subpoena, warrant, or legal demand from any out-of-state authority seeking Colorado resident reproductive health data shall: (a) notify the ODO within twenty-four (24) hours; (b) notify the affected resident within forty-eight (48) hours unless a specific non-disclosure order has been issued; and (c) decline to produce any reproductive health data pending ODO review and Colorado court authorization. The ODO shall challenge any out-of-state demand for Colorado resident reproductive health data as a matter of state public policy.

SECTION 15-15-181. INCAPACITATED ADULT DIGITAL SOUL PROTECTION — COURT-APPOINTED GUARDIAN AUTHORITY — LOCKBOX ACCOUNT — CAPACITY RESTORATION TRANSFER — CONTINUITY OF DIGITAL SOUL RIGHTS

15-15-181. Incapacitated adult Digital Soul — court-appointed guardian or conservator Digital Soul authority — same framework as Minor Digital Soul Trust — lockbox account — no state agency access — capacity restoration transfer — death and intestate provisions apply — CCPAME adult guardianship registry.

(1) Legislative finding. The general assembly finds that Colorado adults who become incapacitated through illness, injury, traumatic brain injury, dementia, or disability retain their Digital Soul property rights — incapacity does not extinguish the property right, it requires a qualified fiduciary to exercise it on the resident's behalf. The same institutional exploitation risks that exist for children in state custody exist for incapacitated adults in care facilities, and the same lockbox protections apply.

(2) Guardian and conservator Digital Soul authority. A Colorado court-appointed guardian or conservator for an adult resident who has been adjudicated incapacitated under C.R.S. §15-14-101 et seq. has the following Digital Soul authority, subject to the limitations of subsection (3): (a) Master Deed registration or maintenance on the incapacitated adult's behalf; (b) Decentralized Identity Verification Protocol consent management — granting, limiting, and revoking covered operator consents; (c) Annual Digital Soul Audit review and Correction Request filing; (d) Universal Telemetry Allowance exercise; (e) ALAM Live Legal Mode activation for Digital Soul violations; and (f) Police Encounter Protocol activation in circumstances where the incapacitated adult is subject to law enforcement interaction.

(3) Lockbox account — identical protections to Minor Digital Soul Trust. The Resident Automated Mitigation Account of a registered incapacitated adult is designated a Locked Adult Digital Soul Account upon adjudication of incapacity and filing of CCPAME notification by the guardian. All provisions of §15-15-162(3) and §15-15-162(4) apply to the Locked Adult Digital Soul Account — including the categorical prohibition on state agency, care facility, and creditor access. The account accrues with full UFIPA compounding. The guardian has no withdrawal authority.

(4) Capacity restoration transfer. Upon a Colorado court's determination that the adult's capacity has been restored: (a) the Locked Adult Digital Soul Account transfers unconditionally to the adult as their sole and separate property; (b) the CCPAME notifies the adult of the transfer amount and provides instructions for full account access; and (c) the guardian's Digital Soul authority automatically terminates. No state agency, care facility, or creditor may claim any portion of the transferred account balance.

SECTION 15-15-182. DATA MINIMIZATION MANDATE — COLLECTION LIMITED TO SERVICE PURPOSE — EXCESS COLLECTION AS TIER 1 VIOLATION — PURPOSE LIMITATION — STORAGE MINIMIZATION

15-15-182. Data minimization mandate — covered operators may collect only Digital Soul reasonably necessary for specific consented service — purpose limitation — storage minimization — excess collection as Tier 1 violation per resident per day — CCPAME minimization standards — annual minimization audit.

(1) Data minimization mandate. A covered operator may collect, process, and retain only those categories of Colorado resident Digital Soul that are: (a) reasonably necessary for the specific service for which the resident has provided Decentralized Identity Verification Protocol consent; and (b) proportionate to the service — the volume and sensitivity of Digital Soul collected must be proportionate to the benefit of the service provided. Collection of Digital Soul beyond what is reasonably necessary for the consented service purpose is a Tier 1 violation for each excess category per resident per day.

(2) Purpose limitation. Digital Soul collected for one service purpose may not be processed for any other purpose without independent DID consent for the new purpose. The purpose limitation is absolute — the covered operator may not rely on any consent to use data for a new purpose not specified in the original consent, regardless of how broadly the original consent was worded. Each instance of purpose-violating processing is a separate violation.

(3) Storage minimization. A covered operator shall delete resident Digital Soul: (a) upon the resident's revocation of consent — within thirty (30) days with cryptographic proof of deletion; (b) when the data is no longer necessary for the specific consented purpose — without requiring resident request; (c) at the end of the retention period specified in the DID consent; and (d) in any event, no later than three (3) years after collection unless the resident has affirmatively renewed consent within the prior twelve (12) months. Failure to delete as required is a Tier 1 violation per record per day after the required deletion date.

(4) CCPAME minimization standards. The CCPAME shall publish Data Minimization Standards for each major industry category of covered operator within eighteen (18) months of enactment, establishing presumptive guidance on what Digital Soul categories are reasonably necessary for common services. Covered operators operating within the published minimization standards for their industry are entitled to a good-faith compliance presumption in any enforcement proceeding.

AMPLIFY ACT v28 — BILL 2 FINAL COMPLETION SECTIONS

§§10-10-308 through 10-10-314

Physical Kill Switch · Sensory Presence Buffer · Silence Right · Choice of Law · Interstate Transfer · Criminal Penalties · Anti-SLAPP · Private AG · Smart Building

---

SECTION 10-10-308. PHYSICAL ISOLATION MECHANISM — SENSORY PRESENCE BUFFER — OWNER'S RIGHT TO SILENCE — HARDWARE CERTIFICATION — DID PREFERENCE PROFILE — PROXIMITY LIABILITY

10-10-308. Physical Isolation Mechanism — mandatory hardwired interrupt — CCPAME hardware certification — Sensory Presence Buffer — presence detection only without consent — no biometric or behavioral processing without DID handshake — Owner's Right to Silence — AI may not initiate contact during declared Silence Period — DID preference profile broadcasting — smart space compliance — $1,000/sensor/day violation — strict operator liability.

(1) Legislative finding. The general assembly finds that: (a) A Colorado resident's right to physical presence without being processed as a data subject is the spatial extension of the Digital Soul property right — a resident in a room containing covered automation systems has the right to be present without being analyzed, identified, or characterized by those systems absent affirmative consent; (b) A hardware-level physical interrupt — not a software command, not a firmware setting, not a network configuration — is the only technically reliable mechanism for ensuring that a covered automation system cannot process resident data when the resident has not consented; software can be overridden by software, hardware cannot be overridden by software; (c) The Owner's Right to Silence — the right of a covered automation system's registered owner to declare a period during which the system does not initiate contact, monitor for trigger phrases, or generate unsolicited output — is a property right in the owner's relationship with their own AI utility, as fundamental as the right to turn off a device; and (d) Every resident who enters a smart space — a hotel room, office, retail environment, healthcare facility, or any other space containing covered automation systems — carries their Digital Soul preferences with them through their Decentralized Identity Verification Protocol credential and is entitled to have those preferences honored automatically.

(2) Physical Isolation Mechanism — mandatory hardware requirement. Every covered automation system operating in a location accessible to Colorado residents shall incorporate a Physical Isolation Mechanism (PIM) meeting the following specifications: (a) The PIM is a hardwired hardware interrupt — operating at the physical layer below all software, firmware, and network layers — that when activated: (I) cuts all sensor input processing including audio, video, thermal, biometric, radar, lidar, and any other sensing modality; (II) cuts all output capability including speakers, displays, haptic outputs, and network transmissions; (III) cuts all actuator control; (IV) cuts all network connectivity; and (V) does not transmit, store, or log any data generated after PIM activation; (b) The PIM cannot be overridden, bypassed, defeated, or reactivated by any software command, remote instruction, firmware update, operator override, or network signal — physical reactivation by an authorized person is the only reactivation mechanism; (c) The PIM is accessible to the resident — the physical activation mechanism is visible, labeled in plain language, and operable without technical knowledge; and (d) The PIM activation status is indicated by a physical indicator — an LED, display, or mechanical indicator — that cannot be spoofed by software.

(3) CCPAME Hardware Certification. The CCPAME shall establish and administer a Hardware Certification program for Physical Isolation Mechanisms: (a) All covered automation systems deployed in Colorado after the effective date of this section shall have CCPAME-certified PIMs before deployment; (b) Existing covered automation systems shall achieve PIM certification within twenty-four (24) months of enactment; (c) Certification requires independent hardware security audit by a CCPAME-approved laboratory — not self-certification; (d) Certification is tamper-evident — any covered operator who disables, bypasses, or modifies a certified PIM forfeits certification and is subject to a Critical Severity Violation; and (e) The CCPAME publishes a public PIM Certification Registry showing all certified devices, certification dates, and certification status on the Public Accountability Dashboard.

(4) Sensory Presence Buffer — presence only, no processing. In the absence of an active Decentralized Identity Verification Protocol consent session, a covered automation system operating in a space occupied by a Colorado resident may: (a) detect occupancy — the presence of one or more persons in a defined space — through proximity sensors, pressure sensors, or other non-biometric means; and (b) adjust environmental controls — lighting, temperature, ventilation — based solely on occupancy, not on the identity or characteristics of the occupant. A covered automation system may not, absent an active DID consent

session: (a) process audio, video, or any other sensory input to identify, characterize, profile, or analyze the resident in any way; (b) activate facial recognition, voiceprint analysis, gait analysis, or any other biometric processing modality; (c) log, store, or transmit any data derived from the resident's physical presence beyond aggregate occupancy counts; or (d) attempt to initiate a DID consent session through sensory processing — a DID consent session may only be initiated by the resident's affirmative action.

(5) DID Preference Profile — smart space automatic compliance. A registered Master Deed holder may configure a Physical Space Preference Profile within their myColorado DID credential specifying: (a) default Sensory Presence Buffer level — from full isolation (presence detection only) to full interaction (complete DID consent session); (b) trusted space designations — spaces where the resident has pre-authorized full interaction; (c) Silence Period schedule — days and times during which the Owner's Right to Silence is automatically active; and (d) emergency override settings — situations where safety monitoring overrides Silence Period. When a resident carrying an active myColorado DID enters a CAEP-compliant smart space, the space's covered automation systems receive the resident's Physical Space Preference Profile and configure automatically — the resident's preferences are honored without any action required by the resident.

(6) Owner's Right to Silence. A registered Master Deed holder has the absolute right to declare a Silence Period — a period during which the owner's AI utility: (a) does not initiate any contact, communication, notification, or alert; (b) does not monitor for trigger phrases, wake words, or activation signals; (c) does not queue, schedule, or log notifications for delivery upon Silence Period expiration; (d) does not process any ambient audio, video, or environmental data; and (e) remains on standby — aware of its operational state but producing no output and processing no input. Silence Period may be invoked: (I) through a single tap in the myColorado application; (II) through a pre-registered physical gesture recognized at the hardware layer before the Silence Period takes effect; (III) through a single voice command that activates the Silence Period and then immediately ceases all audio processing. An AI utility that initiates contact, generates output, or attempts communication during a declared Silence Period commits a breach of the Operator Loyalty Obligation under §10-10-303(6) — strict liability, $1,000 per incident, payable directly to the owner's Resident Automated Mitigation Account.

(7) Smart space residential occupancy — hotel and extended-stay enhanced requirements. Any covered automation system operating within a residential occupancy — including hotels, motels, extended-stay facilities, serviced apartments, and any property where a Colorado resident has resided for thirty (30) or more consecutive days — is subject to: (a) enhanced Sensory Presence Buffer requirements — default to full isolation until the resident affirmatively initiates a DID consent session; (b) mandatory PIM accessibility — the PIM activation mechanism in each residential unit is accessible to the resident, not only to the operator; (c) prohibition on any audio or video recording within the residential unit for any purpose absent a DID consent session — including recording for cleaning schedule optimization, ambient noise monitoring, or any other operational purpose; and (d) written disclosure at check-in of all covered automation systems operating in the resident's unit, the categories of data they are capable of collecting, and instructions for activating the PIM and Silence Period. Non-compliance is a Critical Severity Violation.

(8) Violation — strict operator liability. Violations of this section impose strict liability on the covered operator — the operator cannot claim the covered automation system made an autonomous decision to violate the Sensory Presence Buffer or Silence Period. Damages: one thousand dollars ($1,000) per sensor per day the violation continues, payable directly to

the affected resident's Resident Automated Mitigation Account. The CCPAME may also suspend the covered operator's registration pending PIM recertification.

SECTION 10-10-309. MANDATORY COLORADO VENUE — CHOICE OF LAW PROTECTION — MANDATORY ARBITRATION PROHIBITION — DIGITAL SOUL CLAIMS NON-ARBITRABLE — CLASS ACTION WAIVER VOID

10-10-309. Colorado law governs all Digital Soul claims — contractual choice of law waiver void — mandatory arbitration of Digital Soul claims prohibited — class action waiver void as against public policy — Colorado courts have exclusive jurisdiction — federal arbitration act displacement argument — Digital Soul as statutory property right.

(1) Legislative finding. The general assembly finds that: (a) Covered operator terms of service universally designate Delaware, California, Ireland, or other non-Colorado forums for dispute resolution — routing Colorado residents' Digital Soul claims outside Colorado jurisdiction and effectively nullifying Colorado statutory rights through contractual forum selection; (b) The Supreme Court's decision in AT&T Mobility v. Concepcion, 563 U.S. 333 (2011), made mandatory arbitration clauses with class action waivers nearly unassailable under the Federal Arbitration Act — but the FAA does not preempt state statutes that make specific claims non-arbitrable on public policy grounds when the state legislature expressly so provides; (c) The Digital Soul property right is a Colorado statutory property right created by and enforceable under Colorado law — it does not exist absent this act, and no contract predating or postdating this act can waive a statutory property right created for the public benefit; and (d) Colorado has a compelling public interest in ensuring that the enforcement of Digital Soul property rights occurs in Colorado courts, under Colorado law, with Colorado procedural protections, before Colorado judges familiar with this act's architecture.

(2) Colorado law governs — contractual waiver void. Colorado law governs all claims arising under this act regardless of: (a) any contractual choice-of-law provision designating any other state's or nation's law; (b) the location of the covered operator's principal place of business, servers, or operations; (c) the location of the data processing; or (d) any terms of service, privacy policy, or end-user license agreement provision. Any contractual provision purporting to apply non-Colorado law to a Digital Soul claim arising under this act is void as against public policy and unenforceable in any Colorado proceeding.

(3) Mandatory arbitration prohibition — Digital Soul claims non-arbitrable. Any covered operator provision — in a terms of service, privacy policy, end-user agreement, employment agreement, or any other instrument — that requires a Colorado resident to arbitrate any Digital Soul claim arising under this act is void and unenforceable as a matter of Colorado public policy. The general assembly expressly finds that Digital Soul claims are non-arbitrable because: (a) they arise from a Colorado statutory property right created for the benefit of the public; (b) they involve systemic violations affecting multiple residents simultaneously for which class proceedings are essential; (c) arbitration confidentiality would prevent the Legal Violation Pattern Database from receiving the enforcement data it requires

to function; and (d) arbitrator neutrality cannot be assured when covered operators finance the arbitration industry.

(4) Class action waiver void. Any provision in any instrument between a covered operator and a Colorado resident that purports to waive the resident's right to participate in a class action, class arbitration, or any other collective proceeding for Digital Soul claims arising under this act is void as against public policy. Colorado residents retain the right to proceed collectively regardless of any class action waiver.

(5) Exclusive Colorado court jurisdiction. All Digital Soul claims arising under this act shall be brought in Colorado courts of competent jurisdiction. No Colorado court may transfer, dismiss, or stay a Digital Soul claim on forum non conveniens or any other grounds that would route the claim to a non-Colorado forum. Federal courts applying Colorado law to Digital Soul claims shall apply Colorado's non-arbitrability finding as a state public policy determination.

SECTION 10-10-310. INTERSTATE DATA TRANSFER RESTRICTION — JURISDICTION FOLLOWS THE DATA — OFFSHORE PROCESSING PROHIBITION — DATA TRANSFER CERTIFICATION — SUBSIDIARY ROUTING PROHIBITION

10-10-310. Colorado Digital Soul subject to this act regardless of processing location — covered operator registration is jurisdictional hook — offshore processing without CCPAME Data Transfer Certification prohibited — subsidiary routing to avoid jurisdiction prohibited — foreign government data access restriction — reciprocity framework integration.

(1) Jurisdiction follows the data. Colorado resident Digital Soul is subject to this act and Colorado law regardless of: (a) where the data is stored; (b) where the data is processed; (c) the nationality of the entity processing the data; (d) the corporate structure of the covered operator; or (e) any contractual provision purporting to designate non-Colorado law as governing. The covered operator's Colorado registration — and the Colorado resident's Master Deed registration — are the jurisdictional hooks that travel with the data to any location.

(2) CCPAME Data Transfer Certification — required for offshore processing. A covered operator that processes Colorado resident Digital Soul outside the United States or in any state that the CCPAME has not designated as a reciprocating state under §24-20-167 must obtain a CCPAME Data Transfer Certification: (a) certifying that the offshore or non-reciprocating jurisdiction provides protections at least equivalent to Colorado's for the specific data categories being transferred; (b) contractually binding the offshore processor to Colorado's Digital Soul standards as a condition of data access; (c) establishing that the offshore processor is subject to audit by the CCPAME; and (d) ensuring that Colorado residents retain all Digital Soul rights regardless of the processing location. Processing

Colorado resident Digital Soul offshore without a valid CCPAME Data Transfer Certification is a Critical Severity Violation.

(3) Subsidiary routing prohibition. A covered operator may not route Colorado resident Digital Soul through a subsidiary, affiliate, joint venture, or contractual partner for the purpose of avoiding this act's requirements. Any processing of Colorado resident Digital Soul by any entity under the covered operator's control, direction, or contractual relationship is attributable to the covered operator for purposes of this act — regardless of corporate structure.

(4) Foreign government data access restriction. Colorado resident Digital Soul held by any covered operator — regardless of processing location — may not be accessed by any foreign government, foreign intelligence service, or foreign law enforcement agency without a judicial warrant issued by a Colorado court of competent jurisdiction. A legal demand from a foreign government under any foreign law — including a UK Investigatory Powers Act order, a Chinese Cybersecurity Law data demand, or any other foreign legal mechanism — does not authorize access to Colorado resident Digital Soul. The covered operator shall notify the ODO within twenty-four (24) hours of receiving any foreign government data demand.

SECTION 10-10-311. CRIMINAL PENALTIES — FELONY DIGITAL SOUL VIOLATIONS — CLASS 4 AND CLASS 5 FELONIES — INDIVIDUAL OFFICER AND DIRECTOR LIABILITY — COLORADO CRIMINAL CODE AMENDMENTS

10-10-311. Criminal penalties for intentional Digital Soul violations — under-13 commercial processing Class 4 felony — DNA bankruptcy sale Class 4 felony — Operator Loyalty betrayal Class 5 felony — Physical Isolation Mechanism circumvention Class 5 felony — individual corporate officer liability — Colorado Criminal Code amendment — mens rea requirement — safe harbor for good faith compliance.

(1) Legislative finding. The general assembly finds that civil penalties alone are insufficient deterrence for intentional, high-value Digital Soul violations — when the commercial gain from violation exceeds the expected civil penalty discounted by enforcement probability, rational actors choose to violate. Criminal penalties change the calculus at the board level — corporate officers and directors face personal criminal liability that cannot be indemnified by the corporation, cannot be discharged in bankruptcy, and cannot be transferred to a successor entity.

(2) Class 4 felony violations. The following are Class 4 felonies under C.R.S. §18-1.3-401: (a) Intentional commercial processing of the Digital Soul of a Colorado resident known or reasonably knowable to be under the age of thirteen (13) — each affected minor is a separate count; (b) Intentional sale, transfer, or licensing of Colorado resident DNA or genetic data in any bankruptcy proceeding, asset sale, or corporate transaction, in violation of §15-15-171(5) — each affected resident is a separate count; (c) Intentional transfer of Colorado resident reproductive health data to any law enforcement agency without a

Colorado court warrant, in violation of §15-15-180(3)(a) — each affected resident is a separate count; and (d) Intentional operation of a covered automation system against its registered owner's interests in material breach of the Operator Loyalty Obligation under §10-10-303(6) — where the breach causes actual financial harm exceeding ten thousand dollars ($10,000) to the owner.

(3) Class 5 felony violations. The following are Class 5 felonies under C.R.S. §18-1.3-401: (a) Intentional circumvention, disabling, or bypass of a CCPAME-certified Physical Isolation Mechanism under §10-10-308(3) — each device is a separate count; (b) Intentional deployment of a covered automation system to conduct AI-assisted voter targeting using Colorado Voter Digital Soul in violation of §15-15-170(6) — each targeted voter is a separate count; (c) Intentional operation of a covered automation system using an encryption backdoor in violation of §10-10-303(7); and (d) Intentional filing of a false Annual AI Ethics Disclosure under §10-10-307 that materially misrepresents the covered operator's training data, objective function, or bias audit results.

(4) Individual corporate officer and director liability. For criminal violations under subsections (2) and (3) committed by a covered operator entity: (a) any corporate officer, director, or managing member who directed, authorized, or knowingly permitted the violation is individually criminally liable — corporate form does not shield individual actors; (b) the prosecution need not prove the individual personally executed the violating act — directing, authorizing, or ratifying the act after discovery is sufficient; and (c) corporate indemnification agreements, D&O insurance policies, and employment agreements purporting to indemnify individuals for criminal liability under this act are void as against public policy to the extent they purport to cover criminal fines and restitution.

(5) Good faith compliance safe harbor. A covered operator or individual who: (a) promptly self-reports a violation to the CCPAME before investigation commences; (b) cooperates fully with the ODO investigation; (c) remediates the violation within sixty (60) days; and (d) pays all applicable civil penalties — is entitled to a prosecution declination for the first self-reported violation. The safe harbor is not available for violations involving minor victims, DNA sale, or reproductive health data transfer to law enforcement.

SECTION 10-10-312. ANTI-SLAPP EXPRESS INCORPORATION — STRATEGIC LAWSUIT PROHIBITION — $50,000 MANDATORY DAMAGES — PRIVATE ATTORNEY GENERAL PROVISION — BOUNTY STRUCTURE

10-10-312. Anti-SLAPP express incorporation — covered operator suits against resident Digital Soul rights exercises are SLAPPs — mandatory dismissal with attorney fees and $50,000 damages — private attorney general provision — 15%/25% bounty on multi-resident enforcement recoveries — qui tam mechanism.

(1) Anti-SLAPP express incorporation. Any legal action — civil, administrative, or otherwise — filed by a covered operator or its affiliate against a Colorado resident arising from the resident's exercise of any right under this act is a strategic lawsuit against public

participation (SLAPP) subject to C.R.S. §13-20-1101 et seq. (Colorado's anti-SLAPP statute), as supplemented by this section. Protected activities include: filing a CCPAME complaint; using Live Legal Mode; organizing or joining a Resident Data Cooperative or Farmer Data Cooperative; filing a whistleblower report; submitting a Correction Request; exercising the Universal Telemetry Allowance; activating a Police Encounter Protocol session; and making any public statement about a covered operator's Digital Soul practices. An anti-SLAPP motion shall be filed within sixty (60) days of service of the covered operator's action and shall be heard within thirty (30) days of filing.

(2) Mandatory damages upon SLAPP dismissal. Upon dismissal of a covered operator's action as a SLAPP under this section: (a) the covered operator shall pay the resident's reasonable attorney fees and costs; (b) the covered operator shall pay mandatory statutory damages of fifty thousand dollars ($50,000) per action — not per count, per action; (c) the individual attorneys who filed and prosecuted the SLAPP action are subject to mandatory referral to the Colorado Supreme Court Office of Attorney Regulation Counsel for disciplinary review; and (d) the CCPAME shall note the SLAPP action on the covered operator's Public Accountability Dashboard profile permanently.

(3) Private attorney general provision. A Colorado resident who identifies and brings to successful enforcement a Digital Soul violation affecting multiple residents is entitled to a private attorney general bounty: (a) fifteen percent (15%) of total damages collected where the violation affected one hundred (100) or more residents; (b) twenty-five percent (25%) of total damages collected where the violation affected one thousand (1,000) or more residents. The bounty is paid from enforcement recoveries before remainder flows to affected residents' Resident Automated Mitigation Accounts. Private attorney general actions shall be filed in Colorado courts. Covered operators may not contractually prohibit residents from serving as private attorneys general.

SECTION 10-10-313. PUBLIC HEALTH DATA PROTECTION — EMERGENCY DATA NON-COMMERCIALIZATION — TRIBAL DATA SOVEREIGNTY CONSULTATION — GOVERNMENT-TO-GOVERNMENT PROCESS

10-10-313. Public health emergency data protection — data collected under emergency authorization non-commercial — 90-day post-emergency deletion — AI model training prohibition — tribal data sovereignty — CCPAME government-to-government consultation — tribal Digital Soul framework authority.

(1) Public health emergency data protection. Digital Soul data collected from Colorado residents under any public health emergency authorization — including contact tracing, vaccination records, symptom reporting, quarantine monitoring, and epidemic surveillance — is subject to the following absolute restrictions regardless of any emergency order: (a) may not be used for any commercial purpose including advertising, product development, insurance underwriting, or AI model training; (b) may not be transferred to any non-public-health entity; (c) shall be deleted within ninety (90) days of the end of the declared public health emergency with cryptographic proof of deletion provided to the CCPAME; and (d)

shall never be used to train any AI model for any purpose other than the specific public health function authorized. A covered operator that receives public health emergency data under government contract is bound by these restrictions as a condition of the contract and as a statutory obligation independent of any contract term.

(2) Tribal data sovereignty — government-to-government consultation. The CCPAME shall engage in government-to-government consultation with each federally recognized Native American tribe with members residing in Colorado before: (a) promulgating any rule affecting tribal member Digital Soul data; (b) establishing data transfer certification requirements affecting tribal government operations; (c) designating any tribal territory as a covered operator jurisdiction; and (d) any enforcement action affecting tribal government data systems. Consultation shall occur not fewer than ninety (90) days before any rule takes effect and shall result in a written consultation summary published on the Public Accountability Dashboard.

(3) Tribal Digital Soul framework authority. A federally recognized Colorado tribe may adopt a tribal Digital Soul framework under its sovereign authority that: (a) provides protections at least as comprehensive as this act for tribal member Digital Soul data; (b) establishes a tribal data sovereignty office with CCPAME-equivalent enforcement authority over tribal member data; and (c) enters into a government-to-government data sharing and enforcement cooperation agreement with the CCPAME. Upon adoption of a compliant tribal framework, the tribe's framework governs tribal member Digital Soul data processed on tribal lands — and the CCPAME recognizes the tribal framework as equivalent for interstate reciprocity purposes under §24-20-167.

AMPLIFY ACT v28 — BILL 3 + CROSS-CUTTING FINAL SECTIONS

§§24-20-173 through 24-20-178

Effective Date Staggering · Statutory Damages CPI · Extended SOL · Revenue Waterfall Reconciliation · Regulatory Transition Safe Harbor · Annex E Enforcement Matrix Update

---

SECTION 24-20-173. STAGGERED EFFECTIVE DATES — SEQUENCED IMPLEMENTATION — OPERATIONAL FEASIBILITY — CCPAME BUILD-OUT TIMELINE

24-20-173. Staggered effective dates — sequenced implementation ensuring each system is operational before the next system depends on it — QIEF Day 1 — CCPAME board Day 90 — covered operator registration Month 6 — fee collection Month 12 — Master Deed Registry after quantum certification — ALAM Month 24 — full enforcement Month 30.

(1) Legislative finding. The general assembly finds that simultaneous effective dates across all provisions of this act are operationally infeasible — the enforcement infrastructure must exist before violations can be prosecuted, the Master Deed Registry must be quantum-secure before accepting data, and the CCPAME must be constituted before promulgating rules. Staggered effective dates reflect the logical dependency chain of the act's

implementation and are not a weakening of the act — they are the architecture of a system that works.

(2) Effective date schedule. The provisions of this act take effect according to the following schedule:

(a) Day 1 — Enactment date: (I) Quantum Infrastructure Emergency Fund established — State Treasurer transfer obligation begins; (II) CCPAME establishment authority — Governor authorized to begin appointment process; (III) Physical Isolation Mechanism certification program established — CCPAME may begin accepting hardware for certification; (IV) Attorney General Proposition 117 compliance opinion obligation begins 30-day clock.

(b) Day 90 — Three months post-enactment: (I) CCPAME Board fully constituted — all appointments confirmed; (II) ODO Director appointed; (III) CCPAME rulemaking authority activated; (IV) CCPAME begins publishing on Public Accountability Dashboard.

(c) Month 6 — Six months post-enactment: (I) Covered operator voluntary early registration opens — 10% Year 1 fee discount for operators registering before mandatory registration; (II) Political data operator registration opens; (III) Precision agriculture covered operator registration opens; (IV) CCPAME Data Minimization Standards publication begins.

(d) Month 9 — Nine months post-enactment: (I) Mandatory covered operator registration deadline — all covered operators must register or cease Colorado operations; (II) Regulatory transition safe harbor expires; (III) CCPAME begins civil enforcement for registration violations.

(e) Month 12 — One year post-enactment: (I) Enterprise Mitigation fee collection begins — first quarterly fee assessment; (II) CAMT activated — first revenue deposits; (III) Workforce Transition Account begins accepting applications; (IV) Dark pattern enforcement activated.

(f) Month 18 — Eighteen months post-enactment: (I) QIEF-funded quantum infrastructure must be fully operational — ODO publishes quantum certification; (II) Master Deed Registry opens for resident registration — only after quantum certification published; (III) First Master Deed registrations processed; (IV) Resident Data Cooperative and Farmer Data Cooperative formation authorized.

(g) Month 24 — Two years post-enactment: (I) ALAM goes live — Live Legal Mode, Police Encounter Protocol, Financial Claim Auto-Detection activated for registered Master Deed holders; (II) Annual Digital Soul Audit obligation begins for covered operators — first audits due 60 days after Month 24; (III) Biometric data collection prohibition fully effective for non-CBPA-compliant operators; (IV) Building code whistleblower integration activated in ALAM.

(h) Month 30 — Two and one-half years post-enactment: (I) Full enforcement matrix activated — all Annex E tiers operative; (II) First UFIPA Income Distributions and Resident Mitigation Dividend payments calculated; (III) CCPAME revenue bond authority becomes available — subject to investment-grade rating requirement; (IV) Cross-state reciprocity certification process opens.

(i) Month 36 — Three years post-enactment: (I) First Annual AI Ethics Disclosures due — covered operators who registered at Month 9 file their first full-year disclosure; (II) Post-quantum readiness assessment due from ODO under §10-10-305(3); (III) First Minor Digital Soul Trust transfers to young adults who turned 18 since registration; (IV) Phase 2 constitutional amendment campaign authorized to begin signature collection.

(3) Acceleration authority. If the CCPAME determines that any milestone in subsection (2) can be achieved ahead of schedule, it may accelerate the effective date for that milestone by publishing thirty (30) days advance notice on the Public Accountability Dashboard. No milestone may be delayed beyond the scheduled dates in subsection (2) without a supermajority vote of both chambers under §15-15-168.

SECTION 24-20-174. STATUTORY DAMAGES CPI ADJUSTMENT — ALL DAMAGE FIGURES INFLATION-PROTECTED — EXTENDED DISCOVERY RULE STATUTE OF LIMITATIONS — 5-YEAR SOL FROM AUDIT DISCOVERY

24-20-174. All statutory damages figures in this act adjusted annually by Colorado CPI — same mechanism as fee rate floors — cumulative and ratcheting — extended statute of limitations — 5 years from violation or 3 years from Annual Digital Soul Audit discovery whichever later — tolling during covered operator concealment.

(1) Statutory damages CPI adjustment — universal. All statutory damages figures specified in this act — including but not limited to: the $1,000 and $5,000 per violation CBPA damages under §15-15-175; the $500/record/day correction failure damages under §15-15-176; the $25,000 employee whistleblower retaliation damages under §15-15-177; the $50,000 anti-SLAPP mandatory damages under §10-10-312; the $1,000/sensor/day Sensory Presence Buffer violation damages under §10-10-308; the $10,000/day covered operator penalty under §24-20-159; the $50,000/violation Operator Loyalty Obligation damages under §10-10-303; and all other statutory damages figures in this act — are adjusted annually on January 1 of each year by the Colorado Consumer Price Index for All Urban Consumers, using the same CPI adjustment mechanism as §24-20-156(4). The adjustment is: (a) mandatory — not discretionary; (b) cumulative — each year's adjusted figure compounds on the prior year; and (c) Anti-Dilution Ratchet protected — adjusted figures may only increase, never decrease, without voter approval.

(2) Extended statute of limitations. Notwithstanding any other Colorado limitations period: (a) A Digital Soul claim arising under this act must be brought within five (5) years of the date the violation occurred; or (b) Three (3) years from the date the resident discovered or reasonably should have discovered the violation — including through the Annual Digital Soul Audit under §15-15-172, through an Explanation Notice under §15-15-176, or through CCPAME disclosure — whichever is later. The later of (a) and (b) controls.

(3) Tolling — covered operator concealment. The statute of limitations is tolled during any period in which the covered operator: (a) actively concealed the violation; (b) failed to provide a required Annual Digital Soul Audit that would have revealed the violation; (c) provided a materially false Annual Digital Soul Audit; or (d) failed to respond to a Correction Request that would have revealed the violation. Tolling under this subsection requires a showing that the resident exercised reasonable diligence in discovering the violation.

SECTION 24-20-175. ENTERPRISE MITIGATION REVENUE WATERFALL — COMPLETE RECONCILED DISTRIBUTION ARCHITECTURE — CONFIRMED ARITHMETIC — ALL PROGRAM ACCOUNTS SEQUENCED

24-20-175. Enterprise Mitigation Revenue complete waterfall — confirmed arithmetic — all program account draws reconciled — Overflow Pool calculation — Resident Mitigation Dividend base — waterfall sequence locked — no provision of this act may create a new program account draw without amending this section by supermajority.

(1) Legislative finding. The general assembly finds it essential to publish a single authoritative revenue waterfall reconciling all program account draws established across this act's provisions — ensuring that the Overflow Pool available for resident distributions is calculated correctly and that no individual provision inadvertently creates arithmetic that exceeds 100% of Enterprise Mitigation Revenue.

(2) Authoritative revenue waterfall sequence. Enterprise Mitigation Revenue is distributed in the following sequence — each draw is made before the next layer is calculated:

(a) Layer 1 — QIEF Loan Repayment (first-priority lien until fully repaid): twenty percent (20%) of monthly Enterprise Mitigation Revenue collections until the QIEF emergency loan under §24-20-171 is fully repaid. After full repayment, Layer 1 terminates and all subsequent layers increase proportionally.

(b) Layer 2 — CCPAME Operating Budget: not to exceed eight percent (8%) of annual Enterprise Mitigation Revenue — covers CCPAME staff, ODO operations, Public Accountability Dashboard, ALAM operations, Civic Access Terminal network maintenance, and all other administrative costs.

(c) Layer 3 — Systemic Continuity Reserve: three percent (3%) of annual Enterprise Mitigation Revenue — held in physical instruments under §24-20-161.

(d) Layer 4 — Quantum Infrastructure Maintenance: one percent (1%) of annual Enterprise Mitigation Revenue post-QIEF repayment — ongoing quantum security operations, NIST standard upgrades, and HSM maintenance.

(e) Layer 5 — Workforce Transition Account: five percent (5%) of annual Enterprise Mitigation Revenue under §24-20-168.

(f) Layer 6 — Rural Digital Soul Dividend Reserve: eight percent (8%) of Enterprise Mitigation Revenue attributable to precision agriculture covered operators — not 8% of total revenue; 8% of the agricultural sub-stream only.

(g) Layer 7 — MSMF Child Fund: twenty-five percent (25%) of Enterprise Mitigation Revenue attributable to covered operators whose data processing involves minor Digital Soul — calculated by operator-reported minor user percentage; not 25% of total revenue.

(h) Layer 8 — Investment Reserve mandatory floor: ten percent (10%) of the Overflow Pool (calculated after Layers 1-7) under §24-20-154(2)(a). Note: this draw is from the Overflow Pool, not from gross Enterprise Mitigation Revenue — the arithmetic is sequential, not simultaneous.

(i) Layer 9 — UFIPA Income Distribution: Net Income Receipts of the Investment Reserve distributed annually to all registered Master Deed holders through the UFIPA pipeline.

(j) Layer 10 — Resident Mitigation Dividend: ninety percent (90%) of the Overflow Pool after Layer 8 Investment Reserve draw — distributed to all registered Master Deed holders as the Resident Mitigation Dividend.

(3) Arithmetic confirmation. The general assembly confirms that at base-case revenue: Layers 1-7 draw approximately 17-22% of gross Enterprise Mitigation Revenue (with Layers 6 and 7 calculated on sub-streams, not total revenue). The Overflow Pool is approximately 78-83% of gross Enterprise Mitigation Revenue. Layer 8 draws 10% of the Overflow Pool (approximately 7.8-8.3% of gross revenue). The Resident Mitigation Dividend base is approximately 90% of the Overflow Pool (approximately 70-75% of gross revenue). Total draws do not exceed 100% of gross Enterprise Mitigation Revenue under any scenario modeled in the Fiscal Assumptions.

(4) Waterfall amendment lock. No provision of this act — and no future amendment to this act — may create a new program account draw from Enterprise Mitigation Revenue without: (a) amending this section specifically to add the new draw to the waterfall sequence; (b) providing an updated arithmetic confirmation demonstrating that total draws remain below 100% of gross Enterprise Mitigation Revenue; and (c) receiving a two-thirds supermajority vote of both chambers under §15-15-168. This lock ensures that the waterfall arithmetic remains sound regardless of future legislative additions.

SECTION 24-20-176. REGULATORY TRANSITION SAFE HARBOR — 180-DAY PRE-REGISTRATION SAFE HARBOR — EARLY REGISTRATION DISCOUNT — VOLUNTARY COMPLIANCE INCENTIVES

24-20-176. Regulatory transition safe harbor — 180-day period during which covered operators operating before enactment are not subject to civil penalty for pre-registration operations — voluntary early registration opens Month 6 — 10% Year 1 fee discount for early registrants — safe harbor does not apply to intentional violations — registration obligation still accrues.

(1) Safe harbor period. Covered operators that were operating in Colorado before the enactment of this act are not subject to civil penalty for covered automation activity occurring between the enactment date and the mandatory registration deadline at Month 9 under §24-20-173(2)(d) — provided that the operator: (a) registers with the CCPAME by the Month 9 mandatory deadline; (b) provides complete and accurate registration information; and (c) has not committed any intentional violation of this act during the safe harbor period. The safe harbor is a transitional administrative accommodation — fee obligations accrue from Month 12 regardless of whether the operator registered early or at the mandatory deadline.

(2) Early registration incentive. A covered operator that voluntarily registers with the CCPAME during the Month 6 to Month 9 voluntary registration window under §24-20-

173(2)(c) is entitled to a ten percent (10%) reduction in Enterprise Mitigation fees assessed in Year 1 (Month 12 through Month 24) — reflecting the administrative value of early compliance and the reduced enforcement burden of voluntary registration. The early registration discount applies to base fee rates only and does not apply to any fee premium, surcharge, or multiplier.

(3) Safe harbor exclusions. The safe harbor does not apply to: (a) intentional violations — a covered operator that deliberately violates any provision of this act during the safe harbor period is subject to full civil and criminal penalties for those intentional violations; (b) violations involving minor Digital Soul — the under-13 absolute prohibition under §15-15-174(2) is effective from Day 1 and the safe harbor does not apply; (c) violations involving Voter Digital Soul — Political Data Operator obligations are effective from Month 6 and the safe harbor does not apply after that date; or (d) violations of the Physical Isolation Mechanism requirement — PIM certification must be obtained before any covered automation system is deployed after enactment.

ANNEX E — ENFORCEMENT MATRIX UPDATE — ALL NEW VIOLATION CATEGORIES MAPPED TO ENFORCEMENT TIERS

The following table maps all new violation categories added in v28 final completion sections to the appropriate Annex E enforcement tier. This table supplements and amends Annex E — in the event of conflict, this table controls for the specific violation categories listed.

Violation	Tier	Statutory Damages	Additional Consequences
Biometric data — negligent violation §15-15-175	Tier 2	$1,000/violation (or actual damages if greater)	Class action 3x multiplier for 1,000+ resident scale violations
Biometric data — intentional violation §15-15-175	Tier 3 / Criminal	$5,000/violation + Class 5 felony if intentional at scale	Individual officer criminal liability
Right to Explanation failure §15-15-176	Tier 2	$500/record/day uncorrected after 30-day window	Human review right triggered automatically
Employee Digital Soul consent violation §15-15-177	Tier 2	Standard Tier 2 + private right of action	Whistleblower qui tam 20% of recovery
Employee whistleblower retaliation §15-15-177	Critical	$25,000/incident + mandatory reinstatement + registration suspension	Immediate platform suspension pending remediation
Dark pattern — standard §15-15-173	Tier 2	$500/screen/day	CCPAME Dark Pattern Registry listing
Dark pattern — minor user §15-15-173	Tier 2 Enhanced	$1,500/screen/day	Triple damages — minors receive enhanced protection
Under-13 commercial processing §15-15-174	Critical + Criminal	$10,000/minor/day + Class 4 felony (intentional)	Effective Day 1 — no safe harbor applies

School platform data misuse §15-15-174	Critical	2.0x fee premium + Tier 3 per violation	Contract termination and district notification
Physical Isolation Mechanism circumvention §10-10-308	Critical + Criminal	$1,000/sensor/day + Class 5 felony (intentional)	Mandatory recertification — registration suspended
Sensory Presence Buffer violation §10-10-308	Tier 2	$1,000/sensor/day strict liability	No autonomous AI defense available
Silence Period violation §10-10-308	Tier 1	$1,000/incident to RAMA	Operator Loyalty Obligation breach
Residential occupancy non-disclosure §10-10-308	Tier 2	Standard Tier 2 per unit per day	Critical for hotels/extended-stay
Mandatory arbitration clause deployment §10-10-309	Tier 2	Clause void + $5,000/resident affected	Class action preserved regardless
Interstate data transfer without certification §10-10-310	Critical	Critical Severity per resident per day	Immediate CCPAME registration review
Foreign government data demand non-disclosure §10-10-310	Critical	Critical Severity + AG referral	24-hour ODO notification required
Under-13 DNA sale in bankruptcy §15-15-171	Critical + Criminal	$10,000/record + Class 4 felony	No bankruptcy estate defense
Reproductive health data — law enforcement transfer §15-15-180	Critical + Criminal	$10,000/record + Class 4 felony	Out-of-state warrant not sufficient
SLAPP filing by covered operator §10-10-312	Mandatory dismissal	$50,000/action + attorney fees + disciplinary referral	Permanent Dashboard notation
False AI Ethics Disclosure §10-10-307	Critical + Criminal	Critical Severity + Class 5 felony (intentional)	Individual officer liability
Data minimization excess collection §15-15-182	Tier 1	$500/excess category/resident/day	CCPAME minimization standards provide good faith defense
Agricultural Digital Soul — consent violation §15-15-178	Tier 2	Standard Tier 2 + Rural Dividend restoration	Farmer Data Cooperative standing to enforce
Elder financial exploitation prohibition §15-15-179	Tier 2 Enhanced	Standard Tier 2 x 2 for elder victims	ALAM auto-detection triggers investigation
Public health emergency data commercialization §10-10-313	Critical	Critical Severity + contract termination	Government contractor debarment referral
Voter Digital Soul — AI targeting §15-15-170	Critical + Criminal	$1,000/voter/day + Class 5 felony	Effective from Month 6 registration deadline