

CHAPTER 128

**GOVERNMENT - STATE**

SENATE BILL 11-062

BY SENATOR(S) Cadman, Lambert, Newell, Schwartz, Williams S. ;  
also REPRESENTATIVE(S) Murray, Fields, Holbert, Kerr J., Labuda, Nikkel, Ramirez, Stephens, Wilson.

**AN ACT**

**CONCERNING THE ADMINISTRATIVE DUTIES OF THE OFFICE OF INFORMATION TECHNOLOGY.**

*Be it enacted by the General Assembly of the State of Colorado:*

**SECTION 1.** 24-37.5-104 (7) (h) (II), (7) (h) (III), and (7) (h) (IV), Colorado Revised Statutes, are amended to read:

**24-37.5-104. Transfer of functions - change of name - continuity of existence - legislative declaration - rules.** (7) (h) On and after July 1, 2010, the enterprise facility shall be funded as follows:

(II) For state fiscal year 2011-12, sixty-seven percent by moneys appropriated by the general assembly from the department of state cash fund created in section 24-21-104 (3) (b) and thirty-three percent by moneys appropriated by the general assembly from the ~~computer services~~ INFORMATION TECHNOLOGY revolving fund ~~created~~ ESTABLISHED in ~~section 24-37.5-604 (2)~~ SECTION 24-37.5-112 (1) (a);

(III) For state fiscal year 2012-13, thirty-three percent by moneys appropriated by the general assembly from the department of state cash fund created in section 24-21-104 (3) (b) and sixty-seven percent by moneys appropriated by the general assembly from the ~~computer services~~ INFORMATION TECHNOLOGY revolving fund ~~created~~ ESTABLISHED in ~~section 24-37.5-604 (2)~~ SECTION 24-37.5-112 (1) (a); and

(IV) For state fiscal year 2013-14 and for each state fiscal year thereafter, one hundred percent by moneys appropriated by the general assembly from the ~~computer services~~ INFORMATION TECHNOLOGY revolving fund ~~created~~ ESTABLISHED in ~~section 24-37.5-604 (2)~~ SECTION 24-37.5-112 (1) (a).

---

*Capital letters indicate new material added to existing statutes; dashes through words indicate deletions from existing statutes and such material not part of act.*

**SECTION 2.** 24-37.5-105 (3) (h) and (3) (i), Colorado Revised Statutes, are amended to read:

**24-37.5-105. Office - responsibilities - rules - repeal.** (3) The office shall:

(h) Oversee and supervise the maintenance of INFORMATION, information technology, and the initiation of any information technology updates or projects for state agencies; and

(i) Initiate OR APPROVE all procurements of information technology resources for state agencies and enter into any agreement or contract in connection with such a procurement on behalf of a state agency OR AGENCIES.

**SECTION 3.** 24-37.5-108 (1) (a) and (1) (c), Colorado Revised Statutes, are amended to read:

**24-37.5-108. Statewide communications and information infrastructure - establishment - duties.** (1) With regard to the statewide communications and information infrastructure, the office shall have the following duties:

(a) To ~~review and make recommendations on requirements for~~ ACQUIRE AND MANAGE the statewide communications and information infrastructure based on present and future user applications;

(c) To ~~review and make recommendations related to~~ MANAGE THE ongoing use of the statewide communications and information infrastructure;

**SECTION 4.** 24-37.5-109 (1) (a), Colorado Revised Statutes, is amended to read:

**24-37.5-109. Status of state agencies.** (1) State agencies shall:

(a) Consult with and advise the office on ~~their~~ information technology systems AND REQUIREMENTS;

**SECTION 5.** 24-37.5-402 (9), Colorado Revised Statutes, is amended to read:

**24-37.5-402. Definitions.** As used in this part 4, unless the context otherwise requires:

(9) "Public agency" means every state office, whether ~~legislative~~, executive or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education ~~or the department of higher education~~ OR THE GENERAL ASSEMBLY.

**SECTION 6.** 24-37.5-403 (1), (2) (b), and (3), Colorado Revised Statutes, are amended to read:

**24-37.5-403. Chief information security officer - duties and responsibilities.**

(1) The ~~governor~~ CHIEF INFORMATION OFFICER shall appoint a chief information security officer who shall serve at the pleasure of the ~~governor~~ CHIEF INFORMATION

OFFICER. The SECURITY officer shall report to and be under the supervision of the chief information officer. The SECURITY officer shall exhibit a background and expertise in security and risk management for communications and information resources. In the event the SECURITY officer is unavailable to perform the duties and responsibilities under this part 4, all powers and authority granted to the SECURITY officer may be exercised by the chief information officer.

(2) The chief information security officer shall:

(b) Promulgate rules pursuant to article 4 of this title containing information security policies, standards, and guidelines; ~~for such agencies on or before December 31, 2006;~~

(3) ~~For the state fiscal year commencing on July 1, 2006, the cost of the services provided by the chief information security officer to public agencies in administering this part 4 shall be paid from federal funds received by the state for such purposes. It is the intent of the general assembly that the cost of the services provided by the chief information security officer to a public agency be adequately funded in fiscal years commencing on and after July 1, 2007, through an appropriation to the public agency to pay for such services.~~

**SECTION 7.** 24-37.5-404 (1), (3), (4), (5), and (6), Colorado Revised Statutes, are amended to read:

**24-37.5-404. Public agencies - information security plans.** (1) On or before July 1 ~~2007~~ OF EACH YEAR, each public agency shall develop an information security plan utilizing the information security policies, standards, and guidelines developed by the chief information security officer. The information security plan shall provide information security for the communication and information resources that support the operations and assets of the public agency.

(3) On or before July 15 ~~2007~~ OF EACH YEAR, each public agency shall submit the information security plan developed pursuant to this section to the chief information security officer for approval.

(4) In the event that a public agency fails to submit to the chief information security officer an information security plan on or before July 15 ~~2007~~, OF EACH YEAR or such plan is disapproved by the chief information security officer, the officer shall notify the governor, THE CHIEF INFORMATION OFFICER, and the head ~~and chief information officer~~ of the public agency of noncompliance with this section. If no plan has been approved by September 15 ~~2007~~ OF EACH YEAR, the CHIEF INFORMATION SECURITY officer shall be authorized to temporarily discontinue or suspend the operation of a public agency's communication and information resources until such plan has been submitted to or is approved by the officer.

(5) ~~An information security plan may provide for a phase-in period not to exceed three years. An implementation schedule for the phase-in period shall be included in such a plan. Any phase-in period pursuant to this subsection (5) shall be completed by July 1, 2009.~~

(6) ~~On or before July 1, 2008, and on or before July 1 of each subsequent year,~~

~~the executive director or head of each public agency shall report to the chief information security officer on the development, implementation, and, if applicable, compliance with the phase-in schedule of the public agency's information security plan.~~

**SECTION 8.** 24-37.5-404.5 (1), (2) (e), (3), (5), and (6), Colorado Revised Statutes, are amended to read:

**24-37.5-404.5. Institutions of higher education - information security plans.**

(1) ~~On or before July 1 2007, the department of higher education and~~ OF EACH YEAR, each institution of higher education, in coordination with the department OF HIGHER EDUCATION, shall develop an information security plan. The information security plan shall provide information security for the communication and information resources that support the operations and assets of ~~the department and~~ the institution of higher education.

(2) The information security plan shall include:

(e) A process for detecting, reporting, and responding to security incidents consistent with the information security policy of the institution of higher education. The institutions of higher education, the Colorado commission on higher education, and the chief information security officer shall establish the terms and conditions by which the institutions of higher education ~~and the department of higher education~~ shall report information security incidents to the chief information security officer.

(3) ~~On or before July 15 2007~~ OF EACH YEAR, each institution of higher education shall submit the information security plan developed pursuant to this section to the Colorado commission on higher education for review and comment. The commission shall submit such plans to the chief information security officer.

(5) ~~An information security plan may provide for a phase-in period not to exceed three years. An implementation schedule for the phase-in period shall be included in such a plan. Any phase-in period pursuant to this subsection (5) shall be completed by July 1, 2009.~~

(6) ~~On or before July 1, 2008, and on or before July 1 of each subsequent year, the executive director of the department of higher education shall report to the chief information security officer on the development, implementation, and, if applicable, compliance with the phase-in schedule of the information security plan for each institution of higher education.~~

**SECTION 9.** Part 4 of article 37.5 of title 24, Colorado Revised Statutes, is amended BY THE ADDITION OF A NEW SECTION to read:

**24-37.5-404.7. General assembly - information security plans.** (1) THE GENERAL ASSEMBLY SHALL DEVELOP AN INFORMATION SECURITY PLAN. THE INFORMATION SECURITY PLAN SHALL PROVIDE INFORMATION SECURITY FOR THE COMMUNICATION AND INFORMATION RESOURCES THAT SUPPORT THE OPERATIONS AND ASSETS OF THE GENERAL ASSEMBLY.

(2) THE INFORMATION SECURITY PLAN SHALL INCLUDE:

(a) PERIODIC ASSESSMENTS OF THE RISK AND MAGNITUDE OF THE HARM THAT COULD RESULT FROM A SECURITY INCIDENT;

(b) A PROCESS FOR PROVIDING ADEQUATE INFORMATION SECURITY FOR THE COMMUNICATION AND INFORMATION RESOURCES OF THE GENERAL ASSEMBLY;

(c) INFORMATION SECURITY AWARENESS TRAINING FOR REGULAR EMPLOYEES OF THE GENERAL ASSEMBLY;

(d) PERIODIC TESTING AND EVALUATION OF THE EFFECTIVENESS OF INFORMATION SECURITY FOR THE GENERAL ASSEMBLY, WHICH SHALL BE PERFORMED NOT LESS THAN ANNUALLY;

(e) A PROCESS FOR DETECTING, REPORTING, AND RESPONDING TO SECURITY INCIDENTS CONSISTENT WITH THE INFORMATION SECURITY POLICY OF THE GENERAL ASSEMBLY. THE GENERAL ASSEMBLY AND THE CHIEF INFORMATION SECURITY OFFICER SHALL ESTABLISH THE TERMS AND CONDITIONS BY WHICH THE GENERAL ASSEMBLY SHALL REPORT INFORMATION SECURITY INCIDENTS TO THE CHIEF INFORMATION SECURITY OFFICER.

(f) PLANS AND PROCEDURES TO ENSURE THE CONTINUITY OF OPERATIONS FOR INFORMATION RESOURCES THAT SUPPORT THE OPERATIONS AND ASSETS OF THE GENERAL ASSEMBLY IN THE EVENT OF A SECURITY INCIDENT.

(3) ON OR BEFORE JULY 15 OF EACH YEAR, THE DIRECTOR OF LEGISLATIVE INFORMATION SERVICES FOR THE GENERAL ASSEMBLY SHALL SUBMIT THE INFORMATION SECURITY PLAN DEVELOPED PURSUANT TO THIS SECTION TO THE LEGISLATIVE SERVICE AGENCY DIRECTORS OF THE GENERAL ASSEMBLY FOR REVIEW AND COMMENT. THE LEGISLATIVE SERVICE AGENCY DIRECTORS SHALL SUBMIT SUCH PLAN TO THE CHIEF INFORMATION SECURITY OFFICER.

(4) NOTHING IN THIS SECTION SHALL BE CONSTRUED TO REQUIRE THE GENERAL ASSEMBLY TO ADOPT POLICIES OR STANDARDS THAT CONFLICT WITH FEDERAL LAW, RULES, OR REGULATIONS OR WITH CONTRACTUAL ARRANGEMENTS GOVERNED BY FEDERAL LAWS, RULES, OR REGULATIONS.

(5) THE GENERAL ASSEMBLY SHALL PROVIDE REGULARIZED SECURITY AWARENESS TRAINING TO INFORM THE REGULAR LEGISLATIVE EMPLOYEES, ADMINISTRATORS, AND USERS ABOUT THE INFORMATION SECURITY RISKS AND THE RESPONSIBILITY OF EMPLOYEES, ADMINISTRATORS, AND USERS TO COMPLY WITH THE GENERAL ASSEMBLY'S INFORMATION SECURITY PLAN AND THE POLICIES, STANDARDS, AND PROCEDURES DESIGNED TO REDUCE THOSE RISKS.

**SECTION 10.** 24-37.5-405 (2), Colorado Revised Statutes, is amended to read:

**24-37.5-405. Security incidents - authority of chief information security officer.** (2) The chief information security officer shall be authorized to temporarily discontinue or suspend the operation of a public agency's communication and information resources in order to isolate the source of a security incident. The officer shall give notice to the governor, or the lieutenant governor in the event the governor is not available, ~~and the head and~~ chief information

officer, AND THE HEAD of the public agency concurrent with such discontinuation or suspension of operations. The officer shall ensure, to the extent possible, the continuity of operations for the communication and information resources that support the operations and assets of the public agency.

**SECTION 11. Repeal.** 24-37.5-406, Colorado Revised Statutes, is repealed as follows:

**24-37.5-406. Reporting.** ~~The chief information security officer shall report to the governor and the office on a quarterly basis concerning the implementation of the provisions of this part 4.~~

**SECTION 12.** 24-37.5-502 (3), Colorado Revised Statutes, is amended to read:

**24-37.5-502. Duties and responsibilities.** (3) The chief information officer may enter into contracts with any county, city and county, state agency, private school, school district, board of cooperative educational services, or library and may act as a telecommunications network provider between or among two or more counties or state agencies for the purpose of providing teleconferencing facilities and services between or among such entities, including the judicial system of any county, the department of corrections, and the department of human services and any of their facilities. To assure the availability of such network throughout the various state agencies, private schools, school districts, boards of cooperative educational services, libraries, and counties, ~~the executive director of the department of personnel~~ CHIEF INFORMATION OFFICER shall develop a uniform set of standards for facilities to be utilized by the contracting entities.

**SECTION 13.** 24-37.5-505, Colorado Revised Statutes, is amended to read:

**24-37.5-505. Service charges - pricing policy - repeal.** (1) (a) Users of the office's telephone and data communication services shall be charged the full cost of the particular service, which shall include the cost of all material, labor, and overhead. Said user charges shall be transmitted to the state treasurer, who shall credit the same to the ~~telecommunications~~ INFORMATION TECHNOLOGY revolving fund ~~which fund is hereby created. The moneys in the revolving fund are subject to annual appropriations by the general assembly to the office for use in acquiring such materials, supplies, labor, and overhead as are required for telephone and data communications related service functions~~ CREATED IN SECTION 24-37.5-112. The revolving fund shall include user charges on public safety radio systems of a state agency or other state entity; except that no municipality, county, city and county, or special district shall be charged user charges on public safety radio systems of a state agency or other state entity.

(b) THE FUND BALANCE OF THE TELECOMMUNICATIONS REVOLVING FUND EFFECTIVE THE DAY PRIOR TO THE EFFECTIVE DATE OF THIS PARAGRAPH (b) SHALL BE TRANSFERRED TO THE INFORMATION TECHNOLOGY REVOLVING FUND. THIS PARAGRAPH (b) IS REPEALED, EFFECTIVE JULY 1, 2012.

(2) The chief information officer shall establish a policy of remaining competitive with private industry with regard to the cost, timeliness, and quality of the telephone service or data communication functions provided by the office. ~~Agencies~~

~~interested in purchasing services from the private sector shall work with the office to develop bid specifications, which shall identify all services, requirements, and costs. All bids shall be consistent with the state's long-term telecommunication objectives.~~ AN AGENCY MAY ONLY PURCHASE PRIVATE SERVICES IF IT HAS FIRST WORKED WITH THE OFFICE AND THE OFFICE HAS AUTHORIZED THE PURCHASE OF PRIVATE SERVICES.

**SECTION 14.** 24-37.5-602 (2) (b), Colorado Revised Statutes, is amended to read:

**24-37.5-602. Functions of the GGCC.** (2) (b) ~~The chief information officer of~~ Each agency or department of state government, including institutions of higher education, shall ensure compliance with the policies, standards, and guidelines set forth by the office.

**SECTION 15.** 24-37.5-603 (1) (f), Colorado Revised Statutes, is amended to read:

**24-37.5-603. Powers of the chief information officer - penalty for breach of confidentiality.** (1) In order to perform the functions and duties of the GGCC as set forth in this part 6, the chief information officer shall exercise the following powers:

(f) To control the ~~computer services~~ INFORMATION TECHNOLOGY revolving fund pursuant to ~~section 24-37.5-604~~ SECTION 24-37.5-112.

**SECTION 16.** 24-37.5-604, Colorado Revised Statutes, is amended to read:

**24-37.5-604. Service charges - pricing - repeal.** (1) Users of GGCC services shall be charged by the office the full cost of the particular service, which shall include the cost of all material, labor, equipment, software, services, and overhead. ~~Two months prior to~~ NO LATER THAN the November 1 submission date as required by section 24-37-304, the chief information officer shall establish, publish, and distribute billing rates to user entities and other interested entities effective for the following fiscal year. ~~The billing rates shall not be increased during the fiscal year. User charges shall be paid only out of items of appropriation made specifically for the purchase of services from either the office or from an alternative support source approved by the office. Agencies interested in purchasing services from the private sector shall work with the office to develop bid specifications, which shall identify all services, requirements, and costs. All bids shall be consistent with the state's long-term data processing objectives. The bid process shall be completed so as to coincide with the office's rate publication date.~~

(2) (a) User charges collected under this part 6 shall be transmitted to the state treasurer, who shall credit the same to the ~~computer services~~ INFORMATION TECHNOLOGY revolving fund which fund is hereby created. ~~The moneys in such fund are subject to annual appropriations by the general assembly to the office for the purpose of acquiring such materials, supplies, labor, equipment, software, services, and overhead as are required by the office to supply the services purchased by users~~ CREATED IN SECTION 24-37.5-112.

(b) THE FUND BALANCE OF THE COMPUTER SERVICES REVOLVING FUND EFFECTIVE THE DAY PRIOR TO THE EFFECTIVE DATE OF THIS PARAGRAPH (b) SHALL BE TRANSFERRED TO THE INFORMATION TECHNOLOGY REVOLVING FUND. THIS PARAGRAPH (b) IS REPEALED, EFFECTIVE JULY 1, 2012.

(3) The chief information officer shall establish a policy of remaining competitive with the service provided by private industry with regard to the cost, timeliness, and quality of that service provided by the office. ~~Agencies are encouraged to seek competitive bids from the private sector pursuant to subsection (1) of this section. If the office cannot meet the needs of any agency in any one of the said areas, the agency may seek services elsewhere in consultation with the office.~~ AN AGENCY MAY ONLY PURCHASE PRIVATE SERVICES IF IT HAS FIRST WORKED WITH THE OFFICE AND THE OFFICE HAS AUTHORIZED THE PURCHASE OF PRIVATE SERVICES.

**SECTION 17.** 24-37.5-702 (3), Colorado Revised Statutes, is amended to read:

**24-37.5-702. Definitions.** As used in this part 7, unless the context otherwise requires:

(3) "Data" means ~~unit records~~ THE REPRESENTATION OF FACTS AS TEXTS, NUMBERS, GRAPHICS, IMAGES, SOUNDS, OR VIDEO. FACTS ARE CAPTURED, STORED, AND EXPRESSED AS DATA.

**SECTION 18.** 24-72-202 (6) (b) (X), Colorado Revised Statutes, is amended to read:

**24-72-202. Definitions.** As used in this part 2, unless the context otherwise requires:

(6) (b) "Public records" does not include:

(X) The information security plan of a public agency developed pursuant to section 24-37.5-404 or of ~~the department of higher education~~ or an institution of higher education developed pursuant to section 24-37.5-404.5;

**SECTION 19. 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.

Approved: April 22, 2011