

Kentucky

- (c) of this subsection;
- (e) Public records which are developed by an agency in conjunction with the regulation or supervision of financial institutions, including but not limited to, banks, savings and loan associations, and credit unions, which disclose the agency's internal examining or audit criteria and related analytical methods;
  - (f) The contents of real estate appraisals, engineering or feasibility estimates and evaluations made by or for a public agency relative to acquisition of property, until such time as all of the property has been acquired. The law of eminent domain shall not be affected by this provision;
  - (g) Test questions, scoring keys, and other examination data used to administer a licensing examination, examination for employment, or academic examination before the exam is given or if it is to be given again;
  - (h) Records of law enforcement agencies or agencies involved in administrative adjudication that were compiled in the process of detecting and investigating statutory or regulatory violations if the disclosure of the information would harm the agency by revealing the identity of informants not otherwise known or by premature release of information to be used in a prospective law enforcement action or administrative adjudication. Unless exempted by other provisions of KRS 61.870 to 61.884, public records exempted under this provision shall be open after enforcement action is completed or a decision is made to take no action; however, records or information compiled and maintained by county attorneys or Commonwealth's attorneys pertaining to criminal investigations or criminal litigation shall be exempted from the provisions of KRS 61.870 to 61.884 and shall remain exempted after enforcement action, including litigation, is completed or a decision is made to take no action. The exemptions provided by this subsection shall not be used by the custodian of the records to delay or impede the exercise of rights granted by KRS 61.870 to 61.884;
  - (i) Preliminary drafts, notes, correspondence with private individuals, other than correspondence which is intended to give notice of final action of a public agency;
  - (j) Preliminary recommendations, and preliminary memoranda in which opinions are expressed or policies formulated or recommended;
  - (k) All public records or information the disclosure of which is prohibited by federal law or regulation;
  - (l) Public records or information the disclosure of which is prohibited or restricted or otherwise made confidential by enactment of the General Assembly;
- (m) 1. Public records the disclosure of which would have a reasonable likelihood of threatening the public safety by exposing a vulnerability in preventing, protecting against, mitigating, or responding to a terrorist act and limited to:
- a. Criticality lists resulting from consequence assessments;

Kentucky  
(cont'd)

- b. Vulnerability assessments;
  - c. Antiterrorism protective measures and plans;
  - d. Counterterrorism measures and plans;
  - e. Security and response needs assessments;
  - f. Infrastructure records that expose a vulnerability referred to in this subparagraph through the disclosure of the location, configuration, or security of critical systems, including public utility critical systems. These critical systems shall include but not be limited to information technology, communication, electrical, fire suppression, ventilation, water, wastewater, sewage, and gas systems;
  - g. The following records when their disclosure will expose a vulnerability referred to in this subparagraph: detailed drawings, schematics, maps, or specifications of structural elements, floor plans, and operating, utility, or security systems of any building or facility owned, occupied, leased, or maintained by a public agency; and
  - h. Records when their disclosure will expose a vulnerability referred to in this subparagraph and that describe the exact physical location of hazardous chemical, radiological, or biological materials.
2. As used in this paragraph, "terrorist act" means a criminal act intended to:
    - a. Intimidate or coerce a public agency or all or part of the civilian population;
    - b. Disrupt a system identified in subparagraph 1.f. of this paragraph; or
    - c. Cause massive destruction to a building or facility owned, occupied, leased, or maintained by a public agency.
  3. On the same day that a public agency denies a request to inspect a public record for a reason identified in this paragraph, that public agency shall forward a copy of the written denial of the request, referred to in KRS 61.880(1), to the executive director of the Kentucky Office of Homeland Security and the Attorney General.
  4. Nothing in this paragraph shall affect the obligations of a public agency with respect to disclosure and availability of public records under state environmental, health, and safety programs.
  5. The exemption established in this paragraph shall not apply when a member of the Kentucky General Assembly seeks to inspect a public record identified in this paragraph under the Open Records Law; and
- (n) Public or private records, including books, papers, maps, photographs, cards, tapes, discs, diskettes, recordings, software, or other documentation regardless

## **149.433 Exempting security and infrastructure records.**

(A) As used in this section:

"Act of terrorism" has the same meaning as in section 2909.21 of the Revised Code.

"Express statement" means a written statement substantially similar to the following: "This information is voluntarily submitted to a public office in expectation of protection from disclosure as provided by section 149.433 of the Revised Code."

"Infrastructure record" means any record that discloses the configuration of critical systems including, but not limited to, communication, computer, electrical, mechanical, ventilation, water, and plumbing systems, security codes, or the infrastructure or structural configuration of a building .

"Infrastructure record" includes a risk assessment of infrastructure performed by a state or local law enforcement agency at the request of a property owner or manager.

"Infrastructure record" does not mean a simple floor plan that discloses only the spatial relationship of components of the building .

"Security record" means any of the following:

(1) Any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage;

(2) Any record assembled, prepared, or maintained by a public office or public body to prevent, mitigate, or respond to acts of terrorism, including any of the following:

(a) Those portions of records containing specific and unique vulnerability assessments or specific and unique response plans either of which is intended to prevent or mitigate acts of terrorism, and communication codes or deployment plans of law enforcement or emergency response personnel;

(b) Specific intelligence information and specific investigative records shared by federal and international law enforcement agencies with state and local law enforcement and public safety agencies;

(c) National security records classified under federal executive order and not subject to public disclosure under federal law that are shared by federal agencies, and other records related to national security briefings to assist state and local government with domestic preparedness for acts of terrorism.

(3) An emergency management plan adopted pursuant to section 3313.536 of the Revised Code.

(B)

(1) A record kept by a public office that is a security record is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section.

(2) A record kept by a public office that is an infrastructure record of a public office or a chartered nonpublic school is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section.

(3) A record kept by a public office that is an infrastructure record of a private entity may be exempted from release or disclosure under division (C) of this section.

(C) A record prepared by, submitted to, or kept by a public office that is an infrastructure record of a private entity, which is submitted to the public office for use by the public office, when accompanied by an express statement, is exempt from release or disclosure under section 149.43 of the Revised Code for a period of twenty-five years after its creation if it is retained by the public office for that length of time.

**Section 708. Exceptions for Public Records**

(b) Exceptions- Except as provided in subsections (c) and (d), the following are exempt from access by a requester under this act:

(1) A record the disclosure of which:

- (i) would result in the loss of Federal or State funds by an agency or the Commonwealth; or
- (ii) would be reasonably likely to result in a substantial and demonstrable risk of physical harm to or the personal security of an individual.

(2) A record maintained by an agency in connection with the military, homeland security, national defense, law enforcement or other public safety activity that if disclosed would be reasonably likely to jeopardize or threaten public safety or preparedness or public protection activity or a record that is designated classified by an appropriate Federal or State military authority.

(3) A record, the disclosure of which creates a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system, which may include:

- (i) documents or data relating to computer hardware, source file, software and system networks that could jeopardize computer security by exposing a vulnerability in preventing, protecting against, mitigating or responding to a terrorist act;
- (ii) lists of infrastructure, resources and significant special events, including those defined by the Federal Government in the National Infrastructure Protections, which are deemed critical due to their nature and which result from risk analysis; threat assessments; consequences assessments; antiterrorism protective measures and plans; counterterrorism measures and plans; and security and response needs assessments; and
- (iii) building plans or infrastructure records that expose or create vulnerability through disclosure of the location, configuration or security of critical systems, including public utility systems, structural elements, technology, communication, electrical, fire suppression, ventilation, water, wastewater, sewage and gas systems.

(4) A record regarding computer hardware, software and networks, including administrative or technical records, which, if disclosed would be reasonably likely to jeopardize computer security.

Washington

RCW 42.56.420 Security. The following information relating to security is exempt from disclosure under this chapter: (1) Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of: (a) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and (b) Records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism. (2) Those portions of records containing specific and unique vulnerability assessments or specific and unique emergency and escape response plans at a city, county, or state adult or juvenile correctional facility, the public disclosure of which would have a substantial likelihood of threatening the security of a city, county, or state adult or juvenile correctional facility or any individual's safety; (3) Information compiled by school districts or schools in the development of their comprehensive safe school plans pursuant to RCW 28A.320.125, to the extent that they identify specific vulnerabilities of school districts and each individual school; Public Records Act 29 (4) Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities; and (5) The security section of transportation system safety and security program plans required under RCW 35.21.228, 35A.21.300, 36.01.210, 36.57.120, 36.57A.170, and 81.112.180.