2023 Kansas Statutes

75-7240. Executive branch agency heads; responsibilities related to security of data and information technology resources; reports, confidentiality; training; breach protocol; self-assessment reports. (a) The executive branch agency heads shall:
(1) Be solely responsible for security of all data and information technology resources under such agency's purview, irrespective of the location of the data or resources. Locations of data may include:
(A) Agency sites;
(B) agency real property;
(C) infrastructure in state data centers;
(D) third-party locations; and
(E) in transit between locations;
(2) ensure that an agency-wide information security program is in place;
(3) designate an information security officer to administer the agency's information security program that reports directly to executive leadership;
(4) participate in CISO-sponsored statewide cybersecurity program initiatives and services;
(5) implement policies and standards to ensure that all the agency's data and information technology resources are maintained in compliance with applicable state and federal laws and rules and regulations;
(6) implement appropriate cost-effective safeguards to reduce, eliminate or recover from identified threats to data and information technology resources;
(7) include all appropriate cybersecurity requirements in the agency's request for proposal specifications for procuring data and information technology systems and services;
(8) (A) submit a cybersecurity self-assessment report to the CISO by October 16 of each even-numbered year, including an executive summary of the findings, that assesses the extent to which the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure or inappropriate use;
(B) ensure that the agency conducts annual internal assessments of its security program. Internal assessment results shall be considered confidential and shall not be subject to discovery by or release to any person or agency, outside of the KISO or CISO, without authorization from the executive branch agency director or head; and
(C) prepare or have prepared a financial summary identifying cybersecurity expenditures addressing the findings of the cybersecurity self-assessment report required in subparagraph (A), excluding information that might put the data or information resources of the agency or its contractors at risk and submit such report to the house of representatives committee on appropriations and the senate committee on ways and means; and
(9) ensure that if an agency owns, licenses or maintains computerized data that includes personal information, confidential information or information, the disclosure of which is regulated by law, such agency shall, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:
(A) Comply with the notification requirements set out in K.S.A. 2023 Supp. 50-7a01 et seq., and amendments thereto, and applicable federal laws and rules and regulations, to the same extent as a person who conducts business in this state; and
(B) not later than 48 hours after the discovery of the breach, suspected breach or unauthorized exposure, notify: (i) The CISO; and (ii) if the breach, suspected breach or unauthorized exposure involves election data, the secretary of state.
(b) The director or head of each state agency shall:
(1) Participate in annual agency leadership training to ensure understanding of:
(A) The potential impact of common types of cyberattacks and data breaches on the agency's operations and assets;
(B) how cyberattacks and data breaches on the agency's operations and assets may impact the operations and assets of other governmental entities on the state enterprise network;
(C) how cyberattacks and data breaches occur; and

(D) steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems;
(2) ensure that all information technology login credentials are disabled the same day that any employee ends their employment with the state; and
(3) require that all employees with access to information technology receive a minimum of one hour of information technology security training per year.
(c) (1) The CISO, with input from the joint committee on information technology and the joint committee on Kansas security, shall develop a self-assessment report template for use under subsection (a)(8)(A). The most recent version of such template shall be made available to state agencies prior to July 1 of each even-numbered year. The CISO shall aggregate data from the self-assessments received under subsection (a)(8)(A) and provide a summary of such data to the joint committee on information technology and the joint committee on Kansas security.
(2) Self-assessment reports made to the CISO pursuant to subsection (a)(8)(A) shall be confidential and shall not be subject to the provisions of the Kansas open records act, K.S.A. 45-215 et seq., and amendments thereto. The provisions of this paragraph shall expire on July 1, 2028, unless the legislature reviews and reenacts this provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2028.
History: L. 2018, ch. 97, § 5; L. 2023, ch. 75, § 15; L. 2023, ch. 91, § 6; July 1.
Section was also amended by L. 2023, ch. 25, § 8, but that version was repealed by L. 2023, ch. 91, § 9.