2021 Kansas Statutes

75-7240. Executive branch agency heads; responsibilities; reports; training; breach protocol. The executive branch agency heads shall:

(a) 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: (1) Agency sites; (2) agency real property; (3) infrastructure in state data centers; (4) third-party locations; and (5) in transit between locations;

(b) ensure that an agency-wide information security program is in place;

(c) designate an information security officer to administer the agency's information security program that reports directly to executive leadership;

(d) participate in CISO-sponsored statewide cybersecurity program initiatives and services;

(e) 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;

(f) implement appropriate cost-effective safeguards to reduce, eliminate or recover from identified threats to data and information technology resources;

(g) include all appropriate cybersecurity requirements in the agency's request for proposal specifications for procuring data and information technology systems and services;

(h) (1) submit a cybersecurity 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 a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or the data processing of the agency or of a contractor of 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;

(2) 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. This provision regarding confidentiality shall expire on July 1, 2023, unless the legislature reviews and reenacts such provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2023; and

(3) prepare or have prepared a summary of the cybersecurity assessment report required in paragraph (1), 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 government, technology and security or its successor committee and the senate committee on ways and means;

(i) participate in annual agency leadership training to ensure understanding of: (1) The information and information systems that support the operations and assets of the agency; (2) the potential impact of common types of cyberattacks and data breaches on the agency's operations and assets; (3) how cyberattacks and data breaches on the agency's operations and assets could impact the operations and assets of other governmental entities on the state enterprise network; (4) how cyberattacks and data breaches occur; (5) steps to be undertaken by the executive director or agency head and agency employees to protect their information and information systems; and (6) the annual reporting requirements required of the executive director or agency head; and

(j) 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:

(1) Comply with the notification requirements set out in K.S.A. 2021 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

(2) not later than 48 hours after the discovery of the breach, suspected breach or unauthorized exposure, notify: (A) The CISO; and (B) if the breach, suspected breach or unauthorized exposure involves election data, the secretary of state.

History: L. 2018, ch. 97, § 5; July 1.