2023 Kansas Statutes

75-7244. Significant cybersecurity incidents affecting public entities; notification to Kansas information security office; confidentiality of information. (a) Except as provided in subsection (b):
(1) Any public entity that has a significant cybersecurity incident shall notify the Kansas information security office within 12 hours after discovery of such incident.
(2) Any government contractor that has a significant cybersecurity incident that involves the confidentiality, integrity or availability of personal information or confidential information provided by the state of Kansas, networks or information systems operated by or on behalf of the state of Kansas shall notify the Kansas information security office:
(A) Within 72 hours after the government contractor reasonably believes that such significant cybersecurity incident occurred; or
(B) if a determination is made during the investigation that such information, networks or systems were directly impacted, within 12 hours after such determination is made.
(3) If a significant cybersecurity incident described in paragraph (1) or (2) involves election data, then the public entity or government contractor shall also notify the secretary of state of such incident within the time period required by paragraph (1) or (2).
(b) (1) Any entity that is connected to the Kansas criminal justice information system shall report any cybersecurity incident in accordance with rules and regulations adopted by the Kansas criminal justice information system committee pursuant to K.S.A. 74-5704, and amendments thereto.
(2) An entity that is connected to the Kansas criminal justice information system and is not connected to any other state of Kansas information system shall not be required to make the report required in subsection (a).
(3) The Kansas bureau of investigation shall notify the Kansas information security office of any significant cybersecurity incident report it receives in accordance with rules and regulations adopted pursuant to K.S.A. 74-5704, and amendments thereto, not later than 12 hours after receipt of such report.
(c) (1) The information provided pursuant to this section shall only be shared with individuals who need to know such information for response and defensive activities to preserve the integrity of state information systems and networks or to provide assistance if requested.
(2) Such information shall be confidential and shall not be subject to disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and amendments thereto. This paragraph shall expire on July 1, 2028, unless the legislature reviews and acts to continue such provision pursuant to K.S.A. 45-229, and amendments thereto, prior to July 1, 2028.
(3) The Kansas information security office shall only report the information provided pursuant to this section as aggregate data.
(d) Nothing in this section shall be construed to supersede notification requirements in currently existing contracts between the state of Kansas and entities.
(e) Prior to October 1, 2023, the Kansas information security office shall post instructions on its website for submitting the significant cybersecurity reports required by this section. Such instructions shall include, but not be limited to, the types of incidents that are required to be reported and any information that is required to be included in the report made through the established cybersecurity incident reporting system.
(f) For the purposes of this section:
(1) "Cybersecurity incident" means an event or combination that threatens, without lawful authority, the confidentiality, integrity or availability of information or information systems and that requires an entity to initiate a response or recovery activity;
(2) "entity" means a public entity or government contractor;
(3) "government contractor" means an individual or private entity that performs work for or on behalf of the state of Kansas on a contract basis that has access to or is

hosting state networks, systems, application or information;
(4) "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information;
(5) "personal information" means the same as defined in K.S.A. 2023 Supp. 50-7a01, and amendments thereto;
(6) "private entity" means an individual, corporation, company, partnership, firm, association or other entity that is not a public entity;
(7) "public entity" means any public agency of the state or any political subdivision thereof;
(8) "security breach" means the same as defined in K.S.A. 2023 Supp. 50-7a01, and amendments thereto;
(9) "significant cybersecurity incident" means a cybersecurity incident that results in or is likely to result in financial loss or demonstrable harm to public confidence or public health and safety in the state of Kansas; and
(10) "unauthorized disclosure" means the accidental exposure of personal information to a person or entity that is not authorized or does not have a valid need to view the information.

History: L. 2023, ch. 75, § 1; July 1.