2021 Kansas Statutes

75-7239. Kansas information security office; establishment and administration; separate state agency; powers and duties. (a) There is hereby established within and as a part of the office of information technology services the Kansas information security office. The Kansas information security office shall be administered by the CISO and be staffed appropriately to effect the provisions of the Kansas cybersecurity act.

(b) For the purpose of preparing the governor's budget report and related legislative measures submitted to the legislature, the Kansas information security office, established in this section, shall be considered a separate state agency and shall be titled for such purpose as the "Kansas information security office." The budget estimates and requests of such office shall be presented as from a state agency separate from the department of administration, and such separation shall be maintained in the budget documents and reports prepared by the director of the budget and the governor, or either of them, including all related legislative reports and measures submitted to the legislature.

(c) Under direction of the CISO, the KISO shall:

(1) Administer the Kansas cybersecurity act;

(2) assist the executive branch in developing, implementing and monitoring strategic and comprehensive information security risk-management programs;

(3) facilitate executive branch information security governance, including the consistent application of information security programs, plans and procedures;

(4) using standards adopted by the information technology executive council, create and manage a unified and flexible control framework to integrate and normalize requirements resulting from applicable state and federal laws, and rules and regulations;

(5) facilitate a metrics, logging and reporting framework to measure the efficiency and effectiveness of state information security programs;

(6) provide the executive branch strategic risk guidance for information technology projects, including the evaluation and recommendation of technical controls;

(7) assist in the development of executive branch agency cybersecurity programs that are in compliance with applicable state and federal laws and rules and regulations and standards adopted by the information technology executive council;

(8) coordinate the use of external resources involved in information security programs, including, but not limited to, interviewing and negotiating contracts and fees;

(9) liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure a strong security posture;

(10) assist in the development of plans and procedures to manage and recover business-critical services in the event of a cyberattack or other disaster;

(11) assist executive branch agencies to create a framework for roles and responsibilities relating to information ownership, classification, accountability and protection;

(12) ensure a cybersecurity training program is provided to executive branch agencies at no cost to the agencies;

(13) provide cybersecurity threat briefings to the information technology executive council;

(14) provide an annual status report of executive branch cybersecurity programs of executive branch agencies to the joint committee on information technology and the house committee on government, technology and security; and

(15) perform such other functions and duties as provided by law and as directed by the CISO.

History: L. 2018, ch. 97, § 4; July 1.