

**House Substitute for SENATE BILL No. 291**

By Committee on Legislative Modernization

3-22

1 AN ACT concerning information technology; relating to transferring  
2 cybersecurity employees under the chief information technology officer  
3 of each branch; creating a chief information security officer within the  
4 judicial and legislative branches; requiring the attorney general, Kansas  
5 bureau of investigation, secretary of state, state treasurer and insurance  
6 commissioner to appoint chief information security officers; placing the  
7 duty of cybersecurity under the chief information technology officer;  
8 requiring state agencies to comply with certain minimum cybersecurity  
9 standards; exempting certain audit reports from the open records act  
10 and eliminating the five-year review of such exemption; requiring the  
11 information technology executive council to develop a plan to integrate  
12 all information technology services for the executive branch under the  
13 executive chief information technology officer; making and concerning  
14 appropriations for the fiscal years ending June 30, 2025, and June 30,  
15 2026, for the office of information technology, Kansas information  
16 security office and the adjutant general; authorizing certain transfers  
17 and imposing certain limitations and restrictions and directing or  
18 authorizing certain disbursements and procedures for all state agencies;  
19 requiring legislative review of state agencies not in compliance with  
20 this act; amending K.S.A. 40-110, 75-413, 75-623, 75-710, 75-711 and  
21 75-7203 and K.S.A. 2023 Supp. 45-229, 75-7201, 75-7202, 75-7205,  
22 75-7206, 75-7208, 75-7209, 75-7237, 75-7238, 75-7239 and 75-7240  
23 and repealing the existing sections.  
24

25 *Be it enacted by the Legislature of the State of Kansas:*

26 New Section 1. (a) On and after July 1, 2027, all cybersecurity  
27 services for each branch of state government shall be administered by the  
28 chief information technology officer and the chief information security  
29 officer of such branch. All cybersecurity employees within each branch of  
30 state government shall work at the direction of the chief information  
31 technology officer of the branch. The provisions of this subsection do not  
32 apply to the regents' institutions.

33 (b) Prior to January 1, 2026:

34 (1) The information technology executive council shall develop a  
35 plan to integrate all executive branch information technology services into  
36 the office of information technology services. The council shall consult

1 with each agency head when developing such plan.

2 (2) The judicial chief information technology officer shall develop an  
3 estimated project cost to provide information technology hardware to ~~state~~  
4 ~~and county employees in each judicial district who access applications~~  
5 ~~administered by the judicial branch~~ **{judicial agencies and all employees**  
6 **of such agencies, including state and county-funded judicial branch**  
7 **district court employees}**. Such employees shall be required to use such  
8 state-issued information technology hardware ~~to access such applications~~.  
9 The judicial chief information technology officer shall consult with the  
10 executive chief information technology officer to develop a plan to allow  
11 each piece of information technology hardware that is used to access an  
12 application administered by the judicial branch to be part of the KANWIN  
13 network prior to July 1, 2027.

14 (c) The information technology executive council shall report the  
15 plan developed pursuant to subsection (b) to the senate standing committee  
16 on ways and means and the house standing committee on legislative  
17 modernization or its successor committee prior to January 15, 2026.

18 (d) Prior to February 1, 2025, every website that is maintained by a  
19 branch of government or state agency shall be moved to a ".gov" domain.

20 (e) On July 1, 2025, and each year thereafter, moneys appropriated  
21 from the state general fund to or any special revenue fund of any state  
22 agency for information technology and cybersecurity expenditures shall be  
23 appropriated as a separate line item and shall not be merged with other  
24 items of appropriation for such state agency to allow for detailed review  
25 by the senate committee on ways and means and the house of  
26 representatives committee on appropriations during each regular  
27 legislative session.

28 New Sec. 2. (a) There is hereby established the position of judicial  
29 branch chief information security officer. The judicial chief information  
30 security officer shall be in the unclassified service under the Kansas civil  
31 service act, shall be appointed by the judicial administrator, subject to  
32 approval by the chief justice and shall receive compensation determined  
33 by the judicial administrator, subject to approval of the chief justice.

34 (b) The judicial chief information security officer shall:

35 (1) Report to the judicial administrator;

36 (2) establish security standards and policies to protect the branch's  
37 information technology systems and infrastructure in accordance with  
38 subsection (c);

39 (3) ensure the confidentiality, availability and integrity of the  
40 information transacted, stored or processed in the branch's information  
41 technology systems and infrastructure;

42 (4) develop a centralized cybersecurity protocol for protecting and  
43 managing judicial branch information technology assets and infrastructure;

1 (5) detect and respond to security incidents consistent with  
2 information security standards and policies;

3 (6) be responsible for the cybersecurity of all judicial branch data and  
4 information resources;

5 (7) collaborate with the chief information security officers of the  
6 other branches of state government to respond to cybersecurity incidents;

7 (8) ensure that all justices, judges and judicial branch employees  
8 complete cybersecurity awareness training annually and if an employee  
9 does not complete the required training, such employee's access to any  
10 state-issued hardware or the state network is revoked;

11 (9) review all contracts related to information technology entered into  
12 by a person or entity within the judicial branch to make efforts to reduce  
13 the risk of security vulnerabilities within the supply chain or product and  
14 ensure each contract contains standard security language; and

15 (10) coordinate with the United States cybersecurity and  
16 infrastructure security agency to perform annual audits of judicial branch  
17 agencies for compliance with applicable state and federal laws, rules and  
18 regulations and judicial branch policies and standards. The judicial chief  
19 information security officer shall make an audit request to such agency  
20 annually, regardless of whether or not such agency has the capacity to  
21 perform the requested audit.

22 (c) The judicial chief information security officer shall develop a  
23 cybersecurity program of each judicial agency that complies with the  
24 national institute of standards and technology cybersecurity framework  
25 (CSF) 2.0, as in effect on July 1, 2024. The judicial chief information  
26 security officer shall ensure that such programs achieve a CSF tier of 3.0  
27 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030. The  
28 agency head of each judicial agency shall coordinate with the executive  
29 chief information security officer to achieve such standards.

30 (d) (1) If an audit conducted pursuant to subsection (b)(10) results in  
31 a failure, the judicial chief information security officer shall report such  
32 failure to the speaker of the house of representatives and the president of  
33 the senate within 30 days of receiving notice of such failure. Such report  
34 shall contain a plan to mitigate any security risks identified in the audit.  
35 The judicial chief information security officer shall coordinate for an  
36 additional audit after the mitigation plan is implemented and report the  
37 results of such audit to the speaker of the house of representatives and the  
38 president of the senate.

39 (2) Results of audits conducted pursuant to subsection (b)(10) and the  
40 reports described in subsection (d)(1) shall be confidential and shall not be  
41 subject to discovery or disclosure pursuant to the open records act, K.S.A.  
42 45-215 et seq., and amendments thereto.

43 New Sec. 3. (a) There is hereby established the position of legislative

1 branch chief information security officer. The legislative chief information  
2 security officer shall be in the unclassified service under the Kansas civil  
3 service act, shall be appointed by the legislative coordinating council and  
4 shall receive compensation determined by the legislative coordinating  
5 council.

6 (b) The legislative chief information security officer shall:

7 (1) Report to the legislative chief information technology officer;

8 (2) establish security standards and policies to protect the branch's  
9 information technology systems and infrastructure in accordance with  
10 subsection (c);

11 (3) ensure the confidentiality, availability and integrity of the  
12 information transacted, stored or processed in the branch's information  
13 technology systems and infrastructure;

14 (4) develop a centralized cybersecurity protocol for protecting and  
15 managing legislative branch information technology assets and  
16 infrastructure;

17 (5) detect and respond to security incidents consistent with  
18 information security standards and policies;

19 (6) be responsible for the cybersecurity of all legislative branch data  
20 and information resources and obtain approval from the revisor of statutes  
21 prior to taking any action on any matter that involves a legal issue related  
22 to the security of information technology;

23 (7) collaborate with the chief information security officers of the  
24 other branches of state government to respond to cybersecurity incidents;

25 (8) ensure that all legislators and legislative branch employees  
26 complete cybersecurity awareness training annually and if an employee  
27 does not complete the required training, such employee's access to any  
28 state-issued hardware or the state network is revoked;

29 (9) review all contracts related to information technology entered into  
30 by a person or entity within the legislative branch to make efforts to reduce  
31 the risk of security vulnerabilities within the supply chain or product and  
32 ensure each contract contains standard security language; and

33 (10) coordinate with the United States cybersecurity and  
34 infrastructure security agency to perform annual audits of legislative  
35 branch agencies for compliance with applicable state and federal laws,  
36 rules and regulations and legislative branch policies and standards. The  
37 legislative chief information security officer shall make an audit request to  
38 such agency annually, regardless of whether or not such agency has the  
39 capacity to perform the requested audit.

40 (c) The legislative chief information security officer shall develop a  
41 cybersecurity program of each legislative agency that complies with the  
42 national institute of standards and technology cybersecurity framework  
43 (CSF) 2.0, as in effect on July 1, 2024. The legislative chief information

1 security officer shall ensure that such programs achieve a CSF tier of 3.0  
2 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030. The  
3 agency head of each legislative agency shall coordinate with the legislative  
4 chief information security officer to achieve such standards.

5 (d) (1) If an audit conducted pursuant to subsection (b)(10) results in  
6 a failure, the legislative chief information security officer shall report such  
7 failure to the speaker of the house of representatives and the president of  
8 the senate within 30 days of receiving notice of such failure. Such report  
9 shall contain a plan to mitigate any security risks identified in the audit.  
10 The legislative chief information security officer shall coordinate for an  
11 additional audit after the mitigation plan is implemented and report the  
12 results of such audit to the speaker of the house of representatives and the  
13 president of the senate.

14 (2) Results of audits conducted pursuant to subsection (b)(10) and the  
15 reports described in subsection (d)(1) shall be confidential and shall not be  
16 subject to discovery or disclosure pursuant to the open records act, K.S.A.  
17 45-215 et seq., and amendments thereto.

18 New Sec. 4. (a) On July 1, 2028, and each year thereafter, the director  
19 of the budget, in consultation with the legislative, executive and judicial  
20 chief information technology officers as appropriate, shall determine if  
21 each state agency is in compliance with the provisions of this act for the  
22 previous fiscal year. If the director of the budget determines that a state  
23 agency is not in compliance with the provisions of this act for such fiscal  
24 year, the director shall certify an amount equal to 5% of the amount:

25 (1) Appropriated and reappropriated from the state general fund for  
26 such state agency for such fiscal year; and

27 (2) credited to and available in each special revenue fund for such  
28 state agency in such fiscal year. If during any fiscal year, a special revenue  
29 fund has no expenditure limitation, then an expenditure limitation shall be  
30 established for such fiscal year on such special revenue fund by the  
31 director of the budget in an amount that is 5% less than the amount of  
32 moneys credited to and available in such special revenue fund for such  
33 fiscal year.

34 (b) The director of the budget shall submit a detailed written report to  
35 the legislature on or before the first day of the regular session of the  
36 legislature concerning such compliance determinations, including factors  
37 considered by the director when making such determination, and the  
38 amounts certified for each state agency for such fiscal year.

39 (c) During the regular session of the legislature, the senate committee  
40 on ways and means and the house of representatives committee on  
41 appropriations shall consider such compliance determinations and whether  
42 to lapse amounts appropriated and reappropriated and decrease the  
43 expenditure limitations of special revenue funds for such state agencies

1 during the budget committee hearings for such noncomplying agency.

2 ~~New Sec. 5.~~

3 ~~OFFICE OF INFORMATION TECHNOLOGY SERVICES~~

4 ~~(a) There is appropriated for the above agency from the state general~~  
5 ~~fund for the fiscal year ending June 30, 2026, the following:~~

6 ~~Kansas information~~

7 ~~technology office (335-00-1000).....\$15,000,000~~

8 ~~(b) During fiscal year 2026, the director of the budget, in consultation~~  
9 ~~with the executive branch chief information technology officer and~~  
10 ~~executive branch chief information security officer, shall determine the~~  
11 ~~amount of moneys from the state general fund and each special revenue~~  
12 ~~fund that each executive branch agency has expended during fiscal years~~  
13 ~~2021 through 2025 for services performed by the Kansas information~~  
14 ~~security office or other cybersecurity services for such state agency.~~  
15 ~~Provided, That the director of the budget shall determine such five-year~~  
16 ~~average of each state agency's expenditures from the state general fund and~~  
17 ~~each special revenue fund. Provided further, That during fiscal year 2026,~~  
18 ~~the director of the budget shall certify the amount so determined to the~~  
19 ~~director of accounts and reports and, at the same time as such certification~~  
20 ~~is transmitted to the director of accounts and reports, shall transmit a copy~~  
21 ~~of such certification to the director of legislative research. And provided~~  
22 ~~further, That upon receipt of each such certification, the director of~~  
23 ~~accounts and reports shall: (1) For the amounts from the state general fund,~~  
24 ~~lapse such funds; and (2) for each special revenue fund, transfer the~~  
25 ~~amount from the special revenue fund of the state agency to the~~  
26 ~~information technology security fund established in K.S.A. 75-7239, and~~  
27 ~~amendments thereto.~~

28 ~~New Sec. 6. {5.}~~

29 KANSAS INFORMATION SECURITY OFFICE

30 (a) There is appropriated for the above agency from the following  
31 special revenue fund or funds for the fiscal year ending June 30, 2025, all  
32 moneys now or hereafter lawfully credited to and available in such fund or  
33 funds, except that expenditures other than refunds authorized by law shall  
34 not exceed the following:

35 Information technology security fund.....No limit

36 ~~New Sec. 7. {6.}~~

37 KANSAS INFORMATION SECURITY OFFICE

38 (a) **{There is appropriated for the above agency from the state**  
39 **general fund for the fiscal year ending June 30, 2026, the following:**

40 **Kansas information security office (336-00-1000).....\$15,000,000**

41 (b) }There is appropriated for the above agency from the following  
42 special revenue fund or funds for the fiscal year ending June 30, 2026, all  
43 moneys now or hereafter lawfully credited to and available in such fund or

1 funds, except that expenditures other than refunds authorized by law shall  
 2 not exceed the following:

3 Information technology security fund.....No limit

4 **{(c) During fiscal year 2026, the director of the budget, in**  
 5 **consultation with the executive branch chief information technology**  
 6 **officer and executive branch chief information security officer, shall**  
 7 **determine the amount of moneys from the state general fund and each**  
 8 **special revenue fund that each executive branch agency has expended**  
 9 **during fiscal years 2021 through 2025 for services performed by the**  
 10 **Kansas information security office or other cybersecurity services for**  
 11 **such state agency: *Provided*, That the director of the budget shall**  
 12 **determine such five-year average of each state agency's expenditures**  
 13 **from the state general fund and each special revenue fund: *Provided***  
 14 **further, That during fiscal year 2026, the director of the budget shall**  
 15 **certify the amount so determined to the director of accounts and**  
 16 **reports and, at the same time as such certification is transmitted to the**  
 17 **director of accounts and reports, shall transmit a copy of such**  
 18 **certification to the director of legislative research: *And provided***  
 19 **further, That upon receipt of each such certification, the director of**  
 20 **accounts and reports shall: (1) For the amounts from the state general**  
 21 **fund, lapse such funds; and (2) for each special revenue fund, transfer**  
 22 **the amount from the special revenue fund of the state agency to the**  
 23 **information technology security fund established in K.S.A. 75-7239,**  
 24 **and amendments thereto.}**

25 New Sec. ~~8~~ {7.}

26 ADJUTANT GENERAL

27 (a) There is appropriated for the above agency from the state general  
 28 fund for the fiscal year ending June 30, 2025, the following:

29 Operating expenditures (034-00-1000-0053).....\$250,000

30 *Provided*, That expenditures shall be made by the above agency from such  
 31 account for two full-time employees in the Kansas intelligence fusion  
 32 center to assist in monitoring state information technology systems:  
 33 *Provided further*, That such employees shall be in the unclassified service  
 34 of the civil service act and shall be in addition to the positions of the above  
 35 agency as authorized pursuant to K.S.A. 2023 Supp. 48-3706, and  
 36 amendments thereto.

37 Sec. ~~8~~ {8.} K.S.A. 40-110 is hereby amended to read as follows: 40-

38 110. (a) The commissioner of insurance is hereby authorized to appoint an  
 39 assistant commissioner of insurance, actuaries, two special attorneys who  
 40 shall have been regularly admitted to practice, an executive secretary,  
 41 policy examiners, two field representatives, and a secretary to the  
 42 commissioner. Such appointees shall each receive an annual salary to be  
 43 determined by the commissioner of insurance, within the limits of

1 available appropriations. The commissioner is also authorized to appoint,  
2 within the provisions of the civil service law, and available appropriations,  
3 other employees as necessary to administer the provisions of this act. The  
4 field representatives authorized by this section may be empowered to  
5 conduct inquiries, investigations or to receive complaints. Such field  
6 representatives shall not be empowered to make, or direct to be made, an  
7 examination of the affairs and financial condition of any insurance  
8 company in the process of organization, or applying for admission or  
9 doing business in this state.

10 (b) The appointees authorized by this section shall take the proper  
11 official oath and shall be in no way interested, except as policyholders, in  
12 any insurance company. In the absence of the commissioner of insurance  
13 the assistant commissioner shall perform the duties of the commissioner of  
14 insurance, but shall in all cases execute papers in the name of the  
15 commissioner of insurance, as assistant. The commissioner of insurance  
16 shall be responsible for all acts of an official nature done and performed by  
17 the commissioner's assistant or any person employed in such office. All the  
18 appointees authorized by this section shall hold their office at the will and  
19 pleasure of the commissioner of insurance.

20 (c) *The commissioner shall appoint a chief information security*  
21 *officer who shall be responsible for establishing security standards and*  
22 *policies to protect the department's information technology systems and*  
23 *infrastructure. The chief information security officer shall:*

24 (1) *Develop a cybersecurity program for the department that*  
25 *complies with the national institute of standards and technology*  
26 *cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The chief*  
27 *information security officer shall ensure that such programs achieve a*  
28 *CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1,*  
29 *2030;*

30 (2) *ensure that the commissioner and all employees complete*  
31 *cybersecurity awareness training annually and that if an employee does*  
32 *not complete the required training, such employee's access to any state-*  
33 *issued hardware or the state network is revoked; and*

34 (3) (A) (i) *coordinate with the United States cybersecurity and*  
35 *infrastructure security agency to perform annual audits of the department*  
36 *for compliance with applicable state and federal laws, rules and*  
37 *regulations and department policies and standards; and*

38 (ii) *make an audit request to such agency annually, regardless of*  
39 *whether or not such agency has the capacity to perform the requested*  
40 *audit.*

41 (B) *Results of audits conducted pursuant to this paragraph shall be*  
42 *confidential and shall not be subject to discovery or disclosure pursuant to*  
43 *the open records act, K.S.A. 45-215 et seq., and amendments thereto.*



1       Sec. ~~10~~ {9.} K.S.A. 2023 Supp. 45-229 is hereby amended to read as  
2 follows: 45-229. (a) It is the intent of the legislature that exceptions to  
3 disclosure under the open records act shall be created or maintained only  
4 if:

5       (1) The public record is of a sensitive or personal nature concerning  
6 individuals;

7       (2) the public record is necessary for the effective and efficient  
8 administration of a governmental program; or

9       (3) the public record affects confidential information.

10       The maintenance or creation of an exception to disclosure must be  
11 compelled as measured by these criteria. Further, the legislature finds that  
12 the public has a right to have access to public records unless the criteria in  
13 this section for restricting such access to a public record are met and the  
14 criteria are considered during legislative review in connection with the  
15 particular exception to disclosure to be significant enough to override the  
16 strong public policy of open government. To strengthen the policy of open  
17 government, the legislature shall consider the criteria in this section before  
18 enacting an exception to disclosure.

19       (b) Subject to the provisions of subsections (g) and (h), any new  
20 exception to disclosure or substantial amendment of an existing exception  
21 shall expire on July 1 of the fifth year after enactment of the new  
22 exception or substantial amendment, unless the legislature acts to continue  
23 the exception. A law that enacts a new exception or substantially amends  
24 an existing exception shall state that the exception expires at the end of  
25 five years and that the exception shall be reviewed by the legislature  
26 before the scheduled date.

27       (c) For purposes of this section, an exception is substantially  
28 amended if the amendment expands the scope of the exception to include  
29 more records or information. An exception is not substantially amended if  
30 the amendment narrows the scope of the exception.

31       (d) This section is not intended to repeal an exception that has been  
32 amended following legislative review before the scheduled repeal of the  
33 exception if the exception is not substantially amended as a result of the  
34 review.

35       (e) In the year before the expiration of an exception, the revisor of  
36 statutes shall certify to the president of the senate and the speaker of the  
37 house of representatives, by July 15, the language and statutory citation of  
38 each exception that will expire in the following year that meets the criteria  
39 of an exception as defined in this section. Any exception that is not  
40 identified and certified to the president of the senate and the speaker of the  
41 house of representatives is not subject to legislative review and shall not  
42 expire. If the revisor of statutes fails to certify an exception that the revisor  
43 subsequently determines should have been certified, the revisor shall

1 include the exception in the following year's certification after that  
2 determination.

3 (f) "Exception" means any provision of law that creates an exception  
4 to disclosure or limits disclosure under the open records act pursuant to  
5 K.S.A. 45-221, and amendments thereto, or pursuant to any other  
6 provision of law.

7 (g) A provision of law that creates or amends an exception to  
8 disclosure under the open records law shall not be subject to review and  
9 expiration under this act if such provision:

10 (1) Is required by federal law;

11 (2) applies solely to the legislature or to the state court system;

12 (3) has been reviewed and continued in existence twice by the  
13 legislature; ~~or~~

14 (4) has been reviewed and continued in existence by the legislature  
15 during the 2013 legislative session and thereafter; *or*

16 (5) *is a report of the results of an audit conducted by the United*  
17 *States cybersecurity and infrastructure security agency.*

18 (h) (1) The legislature shall review the exception before its scheduled  
19 expiration and consider as part of the review process the following:

20 (A) What specific records are affected by the exception;

21 (B) whom does the exception uniquely affect, as opposed to the  
22 general public;

23 (C) what is the identifiable public purpose or goal of the exception;

24 (D) whether the information contained in the records may be obtained  
25 readily by alternative means and how it may be obtained;

26 (2) an exception may be created or maintained only if it serves an  
27 identifiable public purpose and may be no broader than is necessary to  
28 meet the public purpose it serves. An identifiable public purpose is served  
29 if the legislature finds that the purpose is sufficiently compelling to  
30 override the strong public policy of open government and cannot be  
31 accomplished without the exception and if the exception:

32 (A) Allows the effective and efficient administration of a  
33 governmental program that would be significantly impaired without the  
34 exception;

35 (B) protects information of a sensitive personal nature concerning  
36 individuals, the release of such information would be defamatory to such  
37 individuals or cause unwarranted damage to the good name or reputation  
38 of such individuals or would jeopardize the safety of such individuals.  
39 Only information that would identify the individuals may be excepted  
40 under this paragraph; or

41 (C) protects information of a confidential nature concerning entities,  
42 including, but not limited to, a formula, pattern, device, combination of  
43 devices, or compilation of information that is used to protect or further a

1 business advantage over those who do not know or use it, if the disclosure  
2 of such information would injure the affected entity in the marketplace.

3 (3) Records made before the date of the expiration of an exception  
4 shall be subject to disclosure as otherwise provided by law. In deciding  
5 whether the records shall be made public, the legislature shall consider  
6 whether the damage or loss to persons or entities uniquely affected by the  
7 exception of the type specified in paragraph (2)(B) or (2)(C) would occur  
8 if the records were made public.

9 (i) (1) Exceptions contained in the following statutes as continued in  
10 existence in section 2 of chapter 126 of the 2005 Session Laws of Kansas  
11 and that have been reviewed and continued in existence twice by the  
12 legislature as provided in subsection (g) are hereby continued in existence:  
13 1-401, 2-1202, 5-512, 9-1137, 9-1712, 9-2217, 10-630, 12-189, 12-1,108,  
14 12-1694, 12-1698, 12-2819, 12-4516, 16-715, 16a-2-304, 17-1312e, 17-  
15 2227, 17-5832, 17-7511, 17-76,139, 19-4321, 21-2511, 22-3711, 22-4707,  
16 22-4909, 22a-243, 22a-244, 23-605, 23-9,312, 25-4161, 25-4165, 31-405,  
17 34-251, 38-2212, 39-709b, 39-719e, 39-934, 39-1434, 39-1704, 40-222,  
18 40-2,156, 40-2c20, 40-2c21, 40-2d20, 40-2d21, 40-409, 40-956, 40-1128,  
19 40-2807, 40-3012, 40-3304, 40-3308, 40-3403b, 40-3421, 40-3613, 40-  
20 3805, 40-4205, 44-510j, 44-550b, 44-594, 44-635, 44-714, 44-817, 44-  
21 1005, 44-1019, 45-221(a)(1) through (43), 46-256, 46-259, 46-2201, 47-  
22 839, 47-844, 47-849, 47-1709, 48-1614, 49-406, 49-427, 55-1,102, 58-  
23 4114, 59-2135, 59-2802, 59-2979, 59-29b79, 60-3333, 60-3336, 65-102b,  
24 65-118, 65-119, 65-153f, 65-170g, 65-177, 65-1,106, 65-1,113, 65-1,116,  
25 65-1,157a, 65-1,163, 65-1,165, 65-1,168, 65-1,169, 65-1,171, 65-1,172,  
26 65-436, 65-445, 65-507, 65-525, 65-531, 65-657, 65-1135, 65-1467, 65-  
27 1627, 65-1831, 65-2422d, 65-2438, 65-2836, 65-2839a, 65-2898a, 65-  
28 3015, 65-3447, 65-34,108, 65-34,126, 65-4019, 65-4922, 65-4925, 65-  
29 5602, 65-5603, 65-6002, 65-6003, 65-6004, 65-6010, 65-67a05, 65-6803,  
30 65-6804, 66-101c, 66-117, 66-151, 66-1,190, 66-1,203, 66-1220a, 66-  
31 2010, 72-2232, 72-3438, 72-6116, 72-6267, 72-9934, 73-1228, 74-2424,  
32 74-2433f, 74-32,419, 74-4905, 74-4909, 74-50,131, 74-5515, 74-7308, 74-  
33 7338, 74-8104, 74-8307, 74-8705, 74-8804, 74-9805, 75-104, 75-712, 75-  
34 7b15, 75-1267, 75-2943, 75-4332, 75-4362, 75-5133, 75-5266, 75-5665,  
35 75-5666, 75-7310, 76-355, 76-359, 76-493, 76-12b11, 76-12c03, 76-3305,  
36 79-1119, 79-1437f, 79-3234, 79-3395, 79-3420, 79-3499, 79-34,113, 79-  
37 3614, 79-3657, 79-4301 and 79-5206.

38 (2) Exceptions contained in the following statutes as certified by the  
39 revisor of statutes to the president of the senate and the speaker of the  
40 house of representatives pursuant to subsection (e) and that have been  
41 reviewed during the 2015 legislative session and continued in existence by  
42 the legislature as provided in subsection (g) are hereby continued in  
43 existence: 17-2036, 40-5301, 45-221(a)(45), (46) and (49), 48-16a10, 58-

1 4616, 60-3351, 72-3415, 74-50,217 and 75-53,105.

2 (j) (1) Exceptions contained in the following statutes as continued in  
3 existence in section 1 of chapter 87 of the 2006 Session Laws of Kansas  
4 and that have been reviewed and continued in existence twice by the  
5 legislature as provided in subsection (g) are hereby continued in existence:  
6 1-501, 9-1303, 12-4516a, 39-970, 65-525, 65-5117, 65-6016, 65-6017 and  
7 74-7508.

8 (2) Exceptions contained in the following statutes as certified by the  
9 revisor of statutes to the president of the senate and the speaker of the  
10 house of representatives pursuant to subsection (e) during 2015 and that  
11 have been reviewed during the 2016 legislative session are hereby  
12 continued in existence: 12-5611, 22-4906, 22-4909, 38-2310, 38-2311, 38-  
13 2326, 40-955, 44-1132, 45-221(a)(10)(F) and (a)(50), 60-3333, 65-4a05,  
14 65-445(g), 65-6154, 71-218, 75-457, 75-712c, 75-723 and 75-7c06.

15 (k) Exceptions contained in the following statutes as certified by the  
16 revisor of statutes to the president of the senate and the speaker of the  
17 house of representatives pursuant to subsection (e) and that have been  
18 reviewed during the 2014 legislative session and continued in existence by  
19 the legislature as provided in subsection (g) are hereby continued in  
20 existence: 1-205, 2-2204, 8-240, 8-247, 8-255c, 8-1324, 8-1325, 12-  
21 17,150, 12-2001, 17-12a607, 38-1008, 38-2209, 40-5006, 40-5108, 41-  
22 2905, 41-2906, 44-706, 44-1518, 45-221(a)(44), (45), (46), (47) and (48),  
23 50-6a11, 65-1,243, 65-16,104, 65-3239, 74-50,184, 74-8134, 74-99b06,  
24 77-503a and 82a-2210.

25 (l) Exceptions contained in the following statutes as certified by the  
26 revisor of statutes to the president of the senate and the speaker of the  
27 house of representatives pursuant to subsection (e) during 2016 and that  
28 have been reviewed during the 2017 legislative session are hereby  
29 continued in existence: 12-5711, 21-2511, 22-4909, 38-2313, 45-221(a)  
30 (51) and (52), 65-516, 65-1505, 74-2012, 74-5607, 74-8745, 74-8752, 74-  
31 8772, 75-7d01, 75-7d05, 75-5133, 75-7427 and 79-3234.

32 (m) Exceptions contained in the following statutes as certified by the  
33 revisor of statutes to the president of the senate and the speaker of the  
34 house of representatives pursuant to subsection (e) during 2012 and that  
35 have been reviewed during the 2013 legislative session and continued in  
36 existence by the legislature as provided in subsection (g) are hereby  
37 continued in existence: 12-5811, 40-222, 40-223j, 40-5007a, 40-5009a,  
38 40-5012a, 65-1685, 65-1695, 65-2838a, 66-1251, 66-1805, 72-8268, 75-  
39 712 and 75-5366.

40 (n) Exceptions contained in the following statutes as certified by the  
41 revisor of statutes to the president of the senate and the speaker of the  
42 house of representatives pursuant to subsection (e) and that have been  
43 reviewed during the 2018 legislative session are hereby continued in

1 existence: 9-513c(c)(2), 39-709, 45-221(a)(26), (53) and (54), 65-6832,  
2 65-6834, 75-7c06 and 75-7c20.

3 (o) Exceptions contained in the following statutes as certified by the  
4 revisor of statutes to the president of the senate and the speaker of the  
5 house of representatives pursuant to subsection (e) that have been  
6 reviewed during the 2019 legislative session are hereby continued in  
7 existence: 21-2511(h)(2), 21-5905(a)(7), 22-2302(b) and (c), 22-2502(d)  
8 and (e), 40-222(k)(7), 44-714(e), 45-221(a)(55), 46-1106(g) regarding 46-  
9 1106(i), 65-2836(i), 65-2839a(c), 65-2842(d), 65-28a05(n), article 6(d) of  
10 65-6230, 72-6314(a) and 74-7047(b).

11 (p) Exceptions contained in the following statutes as certified by the  
12 revisor of statutes to the president of the senate and the speaker of the  
13 house of representatives pursuant to subsection (e) that have been  
14 reviewed during the 2020 legislative session are hereby continued in  
15 existence: 38-2310(c), 40-409(j)(2), 40-6007(a), 45-221(a)(52), 46-1129,  
16 59-29a22(b)(10) and 65-6747.

17 (q) Exceptions contained in the following statutes as certified by the  
18 revisor of statutes to the president of the senate and the speaker of the  
19 house of representatives pursuant to subsection (e) that have been  
20 reviewed during the 2021 legislative session are hereby continued in  
21 existence: 22-2302(c)(4)(J) and (c)(6)(B), 22-2502(e)(4)(J) and (e)(6)(B)  
22 and 65-6111(d)(4).

23 (r) Exceptions contained in the following statutes as certified by the  
24 revisor of statutes to the president of the senate and the speaker of the  
25 house of representatives pursuant to subsection (e) that have been  
26 reviewed during the 2023 legislative session are hereby continued in  
27 existence: 2-3902 and 66-2020.

28 ~~Sec. 11.~~ **{10.}** K.S.A. 75-413 is hereby amended to read as follows:  
29 75-413. (a) The secretary of state may appoint such other assistants and  
30 clerks as may be authorized by law; but the secretary of state shall be  
31 responsible for the proper discharge of the duties of all assistants and  
32 clerks, and they shall hold their offices at the will and pleasure of the  
33 secretary and shall do and perform such general duties as the secretary  
34 may require.

35 (b) *The secretary of state shall appoint a chief information security*  
36 *officer who shall be responsible for establishing security standards and*  
37 *policies to protect the office's information technology systems and*  
38 *infrastructure. The chief information security officer shall:*

39 (1) *Develop a cybersecurity program for the office that complies with*  
40 *the national institute of standards and technology cybersecurity*  
41 *framework (CSF) 2.0, as in effect on July 1, 2024. The chief information*  
42 *security officer shall ensure that such programs achieve a CSF tier of 3.0*  
43 *prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;*

1       (2) *ensure that the secretary of state and all employees complete*  
2 *cybersecurity awareness training annually and that if an employee does*  
3 *not complete the required training, such employee's access to any state-*  
4 *issued hardware or the state network is revoked; and*

5       (3) (A) (i) *coordinate with the United States cybersecurity and*  
6 *infrastructure security agency to perform annual audits of the office for*  
7 *compliance with applicable state and federal laws, rules and regulations*  
8 *and office policies and standards; and*

9       (ii) *make an audit request to such agency annually, regardless of*  
10 *whether or not such agency has the capacity to perform the requested*  
11 *audit.*

12       (B) *Results of audits conducted pursuant to this paragraph shall be*  
13 *confidential and shall not be subject to discovery or disclosure pursuant to*  
14 *the open records act, K.S.A. 45-215 et seq., and amendments thereto.*

15       Sec. ~~12~~ {11.} K.S.A. 75-623 is hereby amended to read as follows:  
16 75-623. (a) *The treasurer shall appoint such other assistants, clerks,*  
17 *bookkeepers, accountants and stenographers as may be authorized by law,*  
18 *each of which persons shall take the oath of office required of public*  
19 *officers. Such persons shall hold their offices at the will and pleasure of*  
20 *the state treasurer.*

21       (b) *The treasurer shall appoint a chief information security officer*  
22 *who shall be responsible for establishing security standards and policies*  
23 *to protect the office's information technology systems and infrastructure.*  
24 *The chief information security officer shall:*

25       (1) *Develop a cybersecurity program for the office that complies with*  
26 *the national institute of standards and technology cybersecurity*  
27 *framework (CSF) 2.0, as in effect on July 1, 2024. The chief information*  
28 *security officer shall ensure that such programs achieve a CSF tier of 3.0*  
29 *prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;*

30       (2) *ensure that the treasurer and all employees complete*  
31 *cybersecurity awareness training annually and that if an employee does*  
32 *not complete the required training, such employee's access to any state-*  
33 *issued hardware or the state network is revoked; and*

34       (3) (A) (i) *coordinate with the United States cybersecurity and*  
35 *infrastructure security agency to perform annual audits of the office for*  
36 *compliance with applicable state and federal laws, rules and regulations*  
37 *and office policies and standards; and*

38       (ii) *make an audit request to such agency annually, regardless of*  
39 *whether or not such agency has the capacity to perform the requested*  
40 *audit.*

41       (B) *Results of audits conducted pursuant to this paragraph shall be*  
42 *confidential and shall not be subject to discovery or disclosure pursuant to*  
43 *the open records act, K.S.A. 45-215 et seq., and amendments thereto.*

1       Sec. ~~12~~ {12.} K.S.A. 75-710 is hereby amended to read as follows:  
2 75-710. (a) The attorney general shall appoint such assistants, clerks, and  
3 stenographers as shall be authorized by law, and who shall hold their office  
4 at the will and pleasure of the attorney general. All fees and allowances  
5 earned by said assistants or any of them, or allowed to them by any statute  
6 or order of court in any civil or criminal case whatsoever, shall be turned  
7 into the general revenue fund of the state treasury, and the vouchers for  
8 their monthly salaries shall not be honored by the director of accounts and  
9 reports until a verified account of the fees collected by them, or either of  
10 them, during the preceding month, has been filed in the director of  
11 accounts and reports' office. Assistants appointed by the attorney general  
12 shall perform the duties and exercise the powers as prescribed by law and  
13 shall perform other duties as prescribed by the attorney general. Assistants  
14 shall act for and exercise the power of the attorney general to the extent  
15 the attorney general delegates them the authority to do so.

16       (b) *The attorney general shall appoint a chief information security*  
17 *officer who shall be responsible for establishing security standards and*  
18 *policies to protect the office's information technology systems and*  
19 *infrastructure. The chief information security officer shall:*

20       (1) *Develop a cybersecurity program for the office that complies with*  
21 *the national institute of standards and technology cybersecurity*  
22 *framework (CSF) 2.0, as in effect on July 1, 2024. The chief information*  
23 *security officer shall ensure that such programs achieve a CSF tier of 3.0*  
24 *prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;*

25       (2) *ensure that the attorney general and all employees complete*  
26 *cybersecurity awareness training annually and that if an employee does*  
27 *not complete the required training, such employee's access to any state-*  
28 *issued hardware or the state network is revoked; and*

29       (3) (A) (i) *coordinate with the United States cybersecurity and*  
30 *infrastructure security agency to perform annual audits of the office for*  
31 *compliance with applicable state and federal laws, rules and regulations*  
32 *and office policies and standards; and*

33       (ii) *make an audit request to such agency annually, regardless of*  
34 *whether or not such agency has the capacity to perform the requested*  
35 *audit.*

36       (B) *Results of audits conducted pursuant to this paragraph shall be*  
37 *confidential and shall not be subject to discovery or disclosure pursuant to*  
38 *the open records act, K.S.A. 45-215 et seq., and amendments thereto.*

39       Sec. ~~13~~ {13.} K.S.A. 75-711 is hereby amended to read as follows:  
40 75-711. (a) There is hereby established, under the jurisdiction of the  
41 attorney general, a division to be known as the Kansas bureau of  
42 investigation. The director of the bureau shall be appointed by the attorney  
43 general, subject to confirmation by the senate as provided in K.S.A. 75-

1 4315b, and amendments thereto, and shall have special training and  
2 qualifications for such position. Except as provided by K.S.A. 46-2601,  
3 and amendments thereto, no person appointed as director shall exercise  
4 any power, duty or function as director until confirmed by the senate. In  
5 accordance with appropriation acts, the director shall appoint agents who  
6 shall be trained in the detection and apprehension of criminals. The  
7 director shall appoint an associate director, and any such assistant directors  
8 from within the agency as are necessary for the efficient operation of the  
9 bureau, who shall have the qualifications and employee benefits, including  
10 longevity, of an agent. The director also may appoint a deputy director  
11 and, in accordance with appropriation acts, such administrative employees  
12 as are necessary for the efficient operation of the bureau. No person shall  
13 be appointed to a position within the Kansas bureau of investigation if the  
14 person has been convicted of a felony.

15 (b) The director, associate director, deputy director, assistant directors  
16 and any assistant attorneys general assigned to the bureau shall be within  
17 the unclassified service under the Kansas civil service act. All other agents  
18 and employees of the bureau shall be in the classified service under the  
19 Kansas civil service act and their compensation shall be determined as  
20 provided in the Kansas civil service act and shall receive actual and  
21 necessary expenses.

22 (c) Any person who was a member of the bureau at the time of  
23 appointment as director, associate director or assistant director, upon the  
24 expiration of their appointment, shall be returned to an unclassified or  
25 regular classified position under the Kansas civil service act with  
26 compensation comparable to and not lower than compensation being  
27 received at the time of appointment to the unclassified service. If all such  
28 possible positions are filled at that time, a temporary additional position  
29 shall be created for the person until a vacancy exists in the position. While  
30 serving in the temporary additional position, the person shall continue to  
31 be a contributing member of the retirement system for the agents of the  
32 Kansas bureau of investigation.

33 (d) Each agent of the bureau shall subscribe to an oath to faithfully  
34 discharge the duties of such agent's office, as is required of other public  
35 officials.

36 (e) *The director shall appoint a chief information security officer who*  
37 *shall be responsible for establishing security standards and policies to*  
38 *protect the bureau's information technology systems and infrastructure.*  
39 *The chief information security officer shall:*

40 (1) *Develop a cybersecurity program for the bureau that complies*  
41 *with the national institute of standards and technology cybersecurity*  
42 *framework (CSF) 2.0, as in effect on July 1, 2024. The chief information*  
43 *security officer shall ensure that such programs achieve a CSF tier of 3.0*



1 *prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1, 2030;*

2 (2) *ensure that the director and all employees complete cybersecurity*  
3 *awareness training annually and that if an employee does not complete the*  
4 *required training, such employee's access to any state-issued hardware or*  
5 *the state network is revoked; and*

6 (3) (A) (i) *coordinate with the United States cybersecurity and*  
7 *infrastructure security agency to perform annual audits of the department*  
8 *for compliance with applicable state and federal laws, rules and*  
9 *regulations and department policies and standards; and*

10 (ii) *make an audit request to such agency annually, regardless of*  
11 *whether or not such agency has the capacity to perform the requested*  
12 *audit.*

13 (B) *Results of audits conducted pursuant to this paragraph shall be*  
14 *confidential and shall not be subject to discovery or disclosure pursuant to*  
15 *the open records act, K.S.A. 45-215 et seq., and amendments thereto.*

16 Sec. ~~15~~ {14.} K.S.A. 2023 Supp. 75-7201 is hereby amended to read  
17 as follows: 75-7201. As used in K.S.A. 75-7201 through 75-7212, and  
18 amendments thereto:

19 (a) "Business risk" means the overall level of risk determined by a  
20 business risk assessment that includes, but is not limited to, cost,  
21 information security and other elements as determined by the information  
22 technology executive council's policies or policies adopted by the judicial  
23 branch or the legislative coordinating council.

24 (b) "Cumulative cost" means the total expenditures, from all sources,  
25 for any information technology project by one or more state agencies to  
26 meet project objectives from project start to project completion or the date  
27 and time the project is terminated if it is not completed.

28 (c) "Executive agency" means any state agency in the executive  
29 branch of government, *including the judicial council but not the elected*  
30 *office agencies.*

31 (d) "Information technology project" means an information  
32 technology effort by a state agency of defined and limited duration that  
33 implements, effects a change in or presents a risk to processes, services,  
34 security, systems, records, data, human resources or architecture.

35 (e) "Information technology project change or overrun" means any  
36 change in:

37 (1) Planned expenditures for an information technology project that  
38 would result in the total authorized cost of the project being increased  
39 above the currently authorized cost of such project by more than 10% of  
40 such currently authorized cost of such project or an established threshold  
41 within the information technology executive council's policies or policies  
42 adopted by the judicial branch or the legislative coordinating council;

43 (2) the scope or project timeline of an information technology project,

1 as such scope or timeline was presented to and reviewed by the joint  
2 committee or the chief information technology officer to whom the project  
3 was submitted pursuant to K.S.A. 75-7209, and amendments thereto, that  
4 is a change of more than 10% or a change that is significant as determined  
5 by the information technology executive council's policies *or policies*  
6 *adopted by the judicial branch or the legislative coordinating council*; or

7 (3) the proposed use of any new or replacement information  
8 technology equipment or in the use of any existing information technology  
9 equipment that has been significantly upgraded.

10 (f) "Joint committee" means the joint committee on information  
11 technology.

12 (g) "Judicial agency" means any state agency in the judicial branch of  
13 government.

14 (h) "Legislative agency" means any state agency in the legislative  
15 branch of government.

16 (i) "Project" means a planned series of events or activities that is  
17 intended to accomplish a specified outcome in a specified time period,  
18 under consistent management direction within a state agency or shared  
19 among two or more state agencies, and that has an identifiable budget for  
20 anticipated expenses.

21 (j) "Project completion" means the date and time when the head of a  
22 state agency having primary responsibility for an information technology  
23 project certifies that the improvement being produced or altered under the  
24 project is ready for operational use.

25 (k) "Project start" means the date and time when a state agency  
26 begins a formal study of a business process or technology concept to  
27 assess the needs of the state agency, determines project feasibility or  
28 prepares an information technology project budget estimate under K.S.A.  
29 75-7209, and amendments thereto.

30 (l) "State agency" means any state office or officer, department,  
31 board, commission, institution or bureau, or any agency, division or unit  
32 thereof.

33 Sec. ~~16~~ **{15}** K.S.A. 2023 Supp. 75-7202 is hereby amended to read  
34 as follows: 75-7202. (a) There is hereby established the information  
35 technology executive council which shall be attached to the office of  
36 information technology services for purposes of administrative functions.

37 (b) (1) The council shall be composed of ~~17~~ 13 voting members as  
38 follows:

- 39 (A) Two cabinet agency heads or such persons' designees;  
40 (B) two noncabinet agency heads or such persons' designees;  
41 (C) the executive chief information technology officer;  
42 (D) ~~the legislative chief information technology officer;~~  
43 (E) ~~the judicial chief information technology officer;~~

1       ~~(F)~~ the chief executive officer of the state board of regents or such  
2 person's designee;

3       ~~(G)~~(E) one representative of cities;

4       ~~(H)~~(F) one representative of counties; the network manager of the  
5 information network of Kansas (INK);

6       ~~(I)~~(G) one representative with background and knowledge in  
7 technology and cybersecurity from the private sector, except that such  
8 representative or such representative's employer shall not be an  
9 information technology or cybersecurity vendor that does business with  
10 the state of Kansas;

11       ~~(J)~~(H) one representative appointed by the Kansas criminal justice  
12 information system committee; and

13       ~~(K)~~ one member of the senate appointed by the president of the senate  
14 or such member's designee;

15       ~~(L)~~ one member of the senate appointed by the minority leader of the  
16 senate or such member's designee;

17       ~~(M)~~ one member of the house of representatives appointed by the  
18 speaker of the house of representatives or such member's designee; and

19       ~~(N)~~ one member of the house of representatives appointed by the  
20 minority leader of the house of representatives or such member's  
21 designee.  
22       (I) two information technology employees from state board of  
23 regents institutions appointed by the board of regents.

24       (2) The chief information technology architect, the legislative chief  
25 information technology officer, the judicial chief information technology  
26 officer, one member of the senate appointed by the president of the senate,  
27 one member of the senate appointed by the minority leader of the senate,  
28 one member of the house of representatives appointed by the speaker of  
29 the house of representatives and one member of the house of  
30 representatives appointed by the minority leader of the house of  
31 representatives shall be a nonvoting member nonvoting members of the  
32 council.

33       (3) The cabinet agency heads, the noncabinet agency heads, the  
34 representative of cities, the representative of counties and the  
35 representative from the private sector shall be appointed by the governor  
36 for a term not to exceed 18 months. Upon expiration of an appointed  
37 member's term, the member shall continue to hold office until the  
38 appointment of a successor. Legislative members shall remain members of  
39 the legislature in order to retain membership on the council and shall serve  
40 until replaced pursuant to this section. Vacancies of members during a term  
41 shall be filled in the same manner as the original appointment only for the  
42 unexpired part of the term. The appointing authority for a member may  
43 remove the member, reappoint the member or substitute another appointee  
for the member at any time. Nonappointed members shall serve ex officio.

1 (c) The chairperson of the council shall be drawn from the chief  
2 information technology officers, with each chief information technology  
3 officer serving a one-year term. The term of chairperson shall rotate  
4 among the chief information technology officers on an annual basis ~~the~~  
5 *executive chief information technology officer.*

6 (d) The council shall hold ~~quarterly~~ *monthly* meetings and hearings in  
7 the city of Topeka or at such other places as the council designates, on call  
8 of the executive chief information technology officer or on request of four  
9 or more members. A quorum of the council shall be ~~nine~~ *seven members.*  
10 All actions of the council shall be taken by a majority of all of the  
11 members of the council.

12 (e) Except for members specified as a designee in subsection (b),  
13 members of the council may not appoint an individual to represent them  
14 on the council and only members of the council may vote.

15 (f) Members of the council shall receive mileage, tolls and parking as  
16 provided in K.S.A. 75-3223, and amendments thereto, for attendance at  
17 any meeting of the council or any subcommittee meeting authorized by the  
18 council.

19 Sec. ~~17~~ {16.} K.S.A. 75-7203 is hereby amended to read as follows:  
20 75-7203. (a) The information technology executive council is hereby  
21 authorized to adopt such policies and rules and regulations as necessary to  
22 implement, administer and enforce the provisions of this act.

23 (b) The council shall:

24 (1) Adopt:

25 (A) Information technology resource policies and procedures and  
26 project management methodologies for all ~~state~~ *executive branch* agencies;

27 (B) an information technology architecture, including  
28 telecommunications systems, networks and equipment, that covers all state  
29 agencies;

30 (C) standards for data management for all ~~state~~ *executive branch*  
31 agencies; and

32 (D) a strategic information technology management plan for the ~~state~~  
33 *executive branch*;

34 (2) provide direction and coordination for the application of the  
35 ~~state's~~ *executive branch's* information technology resources;

36 (3) designate the ownership of information resource processes and the  
37 lead *executive branch* agency for implementation of new technologies and  
38 networks shared by multiple agencies ~~in different branches within the~~  
39 *executive branch* of state government; ~~and~~

40 (4) *develop a plan to integrate all information technology services*  
41 *for the executive branch into the office of information technology services;*  
42 *and*

43 (5) perform such other functions and duties as necessary to carry out

1 the provisions of this act.

2 (c) *The information technology executive council shall report the*  
3 *plan developed under subsection (b)(4) to the senate standing committee*  
4 *on ways and means and the house standing committee on legislative*  
5 *modernization or its successor committee prior to January 15, 2026, in*  
6 *accordance with section 1, and amendments thereto.*

7 Sec. ~~18~~ {17.} K.S.A. 2023 Supp. 75-7205 is hereby amended to read  
8 as follows: 75-7205. (a) There is hereby established within and as a part of  
9 the office of information technology services the position of executive  
10 chief information technology officer. The executive chief information  
11 technology officer shall be in the unclassified service under the Kansas  
12 civil service act, shall be appointed by the governor, and shall receive  
13 compensation in an amount fixed by the governor. The executive chief  
14 information technology officer shall maintain a presence in any cabinet  
15 established by the governor and shall report to the governor.

16 (b) The executive chief information technology officer shall:

17 (1) Review and consult with each executive agency regarding  
18 information technology plans, deviations from the state information  
19 technology architecture, information technology project estimates and  
20 information technology project changes and overruns submitted by such  
21 agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine  
22 whether the agency has complied with:

23 (A) The information technology resource policies and procedures and  
24 project management methodologies adopted by the information technology  
25 executive council;

26 (B) the information technology architecture adopted by the  
27 information technology executive council;

28 (C) the standards for data management adopted by the information  
29 technology executive council; and

30 (D) the strategic information technology management plan adopted  
31 by the information technology executive council;

32 (2) report to the chief information technology architect all deviations  
33 from the state information architecture that are reported to the executive  
34 information technology officer by executive agencies;

35 (3) submit recommendations to the division of the budget as to the  
36 technical and management merit of information technology projects and  
37 information technology project changes and overruns submitted by  
38 executive agencies that are reportable pursuant to K.S.A. 75-7209, and  
39 amendments thereto;

40 (4) monitor executive agencies' compliance with:

41 (A) The information technology resource policies and procedures and  
42 project management methodologies adopted by the information technology  
43 executive council;

1 (B) the information technology architecture adopted by the  
2 information technology executive council;

3 (C) the standards for data management adopted by the information  
4 technology executive council; and

5 (D) the strategic information technology management plan adopted  
6 by the information technology executive council;

7 (5) coordinate implementation of new information technology among  
8 executive agencies and with the judicial and legislative chief information  
9 technology officers;

10 (6) designate the ownership of information resource processes and the  
11 lead agency for implementation of new technologies and networks shared  
12 by multiple agencies within the executive branch of state government; ~~and~~

13 (7) perform such other functions and duties as provided by law or as  
14 directed by the governor;

15 (8) *consult with the appropriate legal counsel on topics related to*  
16 *confidentiality of information, the open records act, K.S.A. 45-215 et seq.,*  
17 *and amendments thereto, the open meetings act, K.S.A. 75-4317 et seq.,*  
18 *and amendments thereto, and any other legal matter related to*  
19 *information technology;*

20 (9) *ensure that each executive agency has the necessary information*  
21 *technology and cybersecurity staff imbedded within the agency to*  
22 *accomplish the agency's duties;*

23 (10) *maintain all third-party data centers at locations within the*  
24 *United States or with companies that are based in the United States; and*

25 (11) *create a database of all electronic devices within the branch and*  
26 *ensure that each device is inventoried, cataloged and tagged within an*  
27 *inventory device.*

28 (c) *An employee of the office of information technology services shall*  
29 *not disclose confidential information of an executive agency. Violation of*  
30 *this subsection is a severity level 5, nonperson felony.*

31 (d) *The executive chief information technology officer may make a*  
32 *request to the adjutant general to permit the Kansas national guard in a*  
33 *state active duty capacity to perform vulnerability assessments or other*  
34 *assessments of the branch for the purpose of enhancing security. During*  
35 *such vulnerability assessments, members performing the assessment shall,*  
36 *to the extent possible, ensure that no harm is done to the systems being*  
37 *assessed. The executive chief information technology officer shall notify*  
38 *the executive agency that owns the information systems being assessed*  
39 *about such assessment and coordinate to mitigate the security risk.*

40 Sec. ~~19~~ {18.} K.S.A. 2023 Supp. 75-7206 is hereby amended to read  
41 as follows: 75-7206. (a) There is hereby established within and as a part of  
42 the office of the state judicial administrator the position of judicial chief  
43 information technology officer. The judicial chief information technology

1 officer shall be appointed by the judicial administrator, subject to approval  
2 of the chief justice, and shall receive compensation determined by the  
3 judicial administrator, subject to approval of the chief justice.

4 (b) The judicial chief information technology officer shall:

5 (1) Review and consult with each judicial agency regarding  
6 information technology plans, deviations from the state information  
7 technology architecture, information technology project estimates and  
8 information technology project changes and overruns ~~submitted by such~~  
9 ~~agency pursuant to K.S.A. 75-7209, and amendments thereto~~; to determine  
10 whether the agency has complied with:

11 ~~(A) The information technology resource policies and procedures and~~  
12 ~~project management methodologies adopted by the information technology~~  
13 ~~executive council;~~

14 ~~(B) the information technology architecture adopted by the~~  
15 ~~information technology executive council;~~

16 ~~(C) the standards for data management adopted by the information~~  
17 ~~technology executive council; and~~

18 ~~(D) the strategic information technology management plan adopted~~  
19 ~~by the information technology executive council *policies and procedures*~~  
20 ~~*adopted by the judicial branch;*~~

21 (2) report to the chief information technology architect all deviations  
22 from the state information architecture that are reported to the judicial  
23 information technology officer by judicial agencies;

24 (3) submit recommendations to the judicial administrator as to the  
25 technical and management merit of information technology projects and  
26 information technology project changes and overruns submitted by judicial  
27 agencies that are reportable pursuant to K.S.A. 75-7209, and amendments  
28 thereto;

29 ~~(4) monitor judicial agencies' compliance with:~~

30 ~~(A) The information technology resource policies and procedures and~~  
31 ~~project management methodologies adopted by the information technology~~  
32 ~~executive council;~~

33 ~~(B) the information technology architecture adopted by the~~  
34 ~~information technology executive council;~~

35 ~~(C) the standards for data management adopted by the information~~  
36 ~~technology executive council; and~~

37 ~~(D) the strategic information technology management plan adopted~~  
38 ~~by the information technology executive council;~~

39 ~~(5)~~(4) coordinate implementation of new information technology  
40 among judicial agencies and with the executive and legislative chief  
41 information technology officers;

42 ~~(6)~~(5) designate the ownership of information resource processes and  
43 the lead agency for implementation of new technologies and networks

1 shared by multiple agencies within the judicial branch of state  
2 government;~~and~~

3 ~~(7)(6)~~ perform such other functions and duties as provided by law or  
4 as directed by the judicial administrator;

5 (7) ensure that each judicial agency has the necessary information  
6 technology and cybersecurity staff imbedded within the agency to  
7 accomplish the agency's duties;

8 (8) maintain all third-party data centers at locations within the  
9 United States or with companies that are based in the United States; and

10 (9) create a database of all electronic devices within the branch and  
11 ensure that each device is inventoried, cataloged and tagged with an  
12 inventory device.

13 (c) An employee of the office of the state judicial administrator shall  
14 not disclose confidential information of a judicial agency. Violation of this  
15 subsection is a severity level 5, nonperson felony.

16 (d) The judicial chief information technology officer may make a  
17 request to the adjutant general to permit the Kansas national guard in a  
18 state active duty capacity to perform vulnerability assessments or other  
19 assessments of the branch for the purpose of enhancing security. During  
20 such vulnerability assessments, members performing the assessment shall,  
21 to the extent possible, ensure that no harm is done to the systems being  
22 assessed. The judicial chief information technology officer shall notify the  
23 judicial agency that owns the information systems being assessed about  
24 such assessment and coordinate to mitigate the security risk.

25 Sec. ~~20~~ {19.} K.S.A. 2023 Supp. 75-7208 is hereby amended to read  
26 as follows: 75-7208. (a) The legislative chief information technology  
27 officer shall:

28 ~~(a)(1)~~ Review and consult with each legislative agency regarding  
29 information technology plans, deviations from the state information  
30 technology architecture, information technology project estimates and  
31 information technology project changes and overruns submitted by such  
32 agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine  
33 whether the agency has complied with the:

34 ~~(1) Information technology resource policies and procedures and~~  
35 ~~project management methodologies adopted by the information technology~~  
36 ~~executive council;~~

37 ~~(2) information technology architecture adopted by the information~~  
38 ~~technology executive council;~~

39 ~~(3) standards for data management adopted by the information~~  
40 ~~technology executive council; and~~

41 ~~(4) strategic information technology management plan adopted by the~~  
42 ~~information technology executive council policies and procedures adopted~~  
43 ~~by the legislative coordinating council;~~



1 (b)(2) report to the chief information technology architect all  
2 deviations from the state information architecture that are reported to the  
3 legislative information technology officer by legislative agencies;

4 (e)(3) submit recommendations to the legislative coordinating council  
5 as to the technical and management merit of information technology  
6 projects and information technology project changes and overruns  
7 submitted by legislative agencies that are reportable pursuant to K.S.A. 75-  
8 7209, and amendments thereto;

9 (d) ~~monitor legislative agencies' compliance with the:~~

10 (1) ~~Information technology resource policies and procedures and~~  
11 ~~project management methodologies adopted by the information technology~~  
12 ~~executive council;~~

13 (2) ~~information technology architecture adopted by the information~~  
14 ~~technology executive council;~~

15 (3) ~~standards for data management adopted by the information~~  
16 ~~technology executive council; and~~

17 (4) ~~strategic information technology management plan adopted by the~~  
18 ~~information technology executive council;~~

19 (e)(4) coordinate implementation of new information technology  
20 among legislative agencies and with the executive and judicial chief  
21 information technology officers;

22 (f)(5) designate the ownership of information resource processes and  
23 the lead agency for implementation of new technologies and networks  
24 shared by multiple agencies within the legislative branch of state  
25 government;

26 (g)(6) serve as staff of the joint committee; ~~and~~

27 (h)(7) perform such other functions and duties as provided by law or  
28 as directed by the legislative coordinating council or the joint committee;

29 (8) *consult and obtain approval from the revisor of statutes prior to*  
30 *taking action on topics related to confidentiality of information, the open*  
31 *records act, K.S.A. 45-215 et seq., and amendments thereto, the open*  
32 *meetings act, K.S.A. 75-4317 et seq., and amendments thereto, and any*  
33 *other legal matter related to information technology;*

34 (9) *ensure that each legislative agency has the necessary information*  
35 *technology and cybersecurity staff imbedded within the agency to*  
36 *accomplish the agency's duties;*

37 (10) *maintain all third-party data centers at locations within the*  
38 *United States or with companies that are based in the United States;*

39 (11) *create a database of all electronic devices within the branch and*  
40 *ensure that each device is inventoried, cataloged and tagged with an*  
41 *inventory device; and*

42 (12) *set standards for the legislative division of post audit to use*  
43 *when conducting information technology audits that are subject to*

1 approval by the legislative coordinating council.

2 (b) An employee of the Kansas legislative office of information  
3 services or the division of legislative administrative services shall not  
4 disclose confidential information of a legislative agency. Violation of this  
5 subsection is a severity level 5, nonperson felony.

6 (c) The legislative chief information technology officer may make a  
7 request to the adjutant general to permit the Kansas national guard in a  
8 state active duty capacity to perform vulnerability assessments or other  
9 assessments of the branch for the purpose of enhancing security. During  
10 such vulnerability assessments, members performing the assessment shall,  
11 to the extent possible, ensure that no harm is done to the systems being  
12 assessed. The legislative chief information technology officer shall notify  
13 the legislative agency that owns the information systems being assessed  
14 about such assessment and coordinate to mitigate the security risk.

15 Sec. ~~21~~ {20.} K.S.A. 2023 Supp. 75-7209 is hereby amended to read  
16 as follows: 75-7209. (a) (1) Whenever an agency proposes an information  
17 technology project, such agency shall prepare and submit information  
18 technology project documentation to the chief information technology  
19 officer of the branch of state government of which the agency is a part.  
20 Such information technology project documentation shall:

21 (A) Include a financial plan showing the proposed source of funding  
22 and categorized expenditures for each phase of the project and cost  
23 estimates for any needs analyses or other investigations, consulting or  
24 other professional services, computer programs, data, equipment, buildings  
25 or major repairs or improvements to buildings and other items or services  
26 necessary for the project; and

27 (B) be consistent with:

28 (i) Information technology resource policies and procedures and  
29 project management methodologies for all state agencies;

30 (ii) an information technology architecture, including  
31 telecommunications systems, networks and equipment, that covers all state  
32 agencies;

33 (iii) standards for data management for all state agencies; and

34 (iv) a strategic information technology management plan for the state.

35 (2) Any information technology project with significant business risk,  
36 as determined pursuant to the information technology executive council's  
37 policies or policies adopted by the judicial branch or the legislative  
38 coordinating council, shall be presented to the joint committee on  
39 information technology by such branch chief information technology  
40 officer.

41 (b) (1) Prior to the release of any request for proposal for an  
42 information technology project with significant business risk:

43 (A) Specifications for bids or proposals for such project shall be

1 submitted to the chief information technology officer of the branch of state  
2 government of which the agency or agencies are a part. Information  
3 technology projects requiring chief information technology officer  
4 approval shall also require the chief information technology officer's  
5 written approval on specifications for bids or proposals; and

6 (B) (i) The chief information technology officer of the appropriate  
7 branch over the state agency or agencies that are involved in such project  
8 shall submit the project, the project plan, including the architecture, and  
9 the cost-benefit analysis to the joint committee on information technology  
10 to advise and consult on the project. Such chief information technology  
11 officer shall submit such information to each member of the joint  
12 committee and to the director of the legislative research department. Each  
13 such project plan summary shall include a notice specifying the date the  
14 summary was mailed or emailed. After receiving any such project plan  
15 summary, each member shall review the information and may submit  
16 questions, requests for additional information or request a presentation and  
17 review of the proposed project at a meeting of the joint committee. If two  
18 or more members of the joint committee contact the director of the  
19 legislative research department within seven business days of the date  
20 specified in the summary description and request that the joint committee  
21 schedule a meeting for such presentation and review, then the director of  
22 the legislative research department shall notify the chief information  
23 technology officer of the appropriate branch, the head of such agency and  
24 the chairperson of the joint committee that a meeting has been requested  
25 for such presentation and review on the next business day following the  
26 members' contact with the director of the legislative research department.  
27 Upon receiving such notification, the chairperson shall call a meeting of  
28 the joint committee as soon as practicable for the purpose of such  
29 presentation and review and shall furnish the chief information technology  
30 officer of the appropriate branch and the head of such agency with notice  
31 of the time, date and place of the meeting. Except as provided in  
32 subsection (b)(1)(B)(ii), the state agency shall not authorize or approve the  
33 release of any request for proposal or other bid event for an information  
34 technology project without having first advised and consulted with the  
35 joint committee at a meeting.

36 (ii) The state agency or agencies shall be deemed to have advised and  
37 consulted with the joint committee about such proposed release of any  
38 request for proposal or other bid event for an information technology  
39 project and may authorize or approve such proposed release of any request  
40 for proposal or other bid event for an information technology project if:

41 (a) Fewer than two members of the joint committee contact the  
42 director of the legislative research department within seven business days  
43 of the date the project plan summary was mailed and request a committee

1 meeting for a presentation and review of any such proposed request for  
2 proposal or other bid event for an information technology project; or

3 (b) a committee meeting is requested by at least two members of the  
4 joint committee pursuant to this paragraph, but such meeting does not  
5 occur within two calendar weeks of the chairperson receiving the  
6 notification from the director of the legislative research department of a  
7 request for such meeting.

8 (2) (A) Agencies are prohibited from contracting with a vendor to  
9 implement the project if that vendor prepared or assisted in the preparation  
10 of the program statement, the project planning documents or any other  
11 project plans prepared prior to the project being approved by the chief  
12 information technology officer as required by this section.

13 (B) Information technology projects with an estimated cumulative  
14 cost of less than \$5,000,000 are exempted from the provisions of  
15 subparagraph (A).

16 (C) The provisions of subparagraph (A) may be waived with prior  
17 written permission from the chief information technology officer.

18 (c) Annually at the time specified by the chief information technology  
19 officer of the branch of state government of which the agency is a part,  
20 each agency shall submit to such officer:

21 (1) A copy of a three-year strategic information technology plan that  
22 sets forth the agency's current and future information technology needs  
23 and utilization plans for the next three ensuing fiscal years, in such form  
24 and containing such additional information as prescribed by the chief  
25 information technology officer; and

26 (2) any deviations from the state information technology architecture  
27 adopted by the information technology executive council.

28 (d) The provisions of this section shall not apply to the information  
29 network of Kansas (INK).

30 Sec. ~~22~~ {21.} K.S.A. 2023 Supp. 75-7237 is hereby amended to read  
31 as follows: 75-7237. As used in K.S.A. 75-7236 through 75-7243, and  
32 amendments thereto:

33 (a) "Act" means the Kansas cybersecurity act.

34 (b) "Breach" or "breach of security" means unauthorized access of  
35 data in electronic form containing personal information. Good faith access  
36 of personal information by an employee or agent of an executive branch  
37 agency does not constitute a breach of security, provided that the  
38 information is not used for a purpose unrelated to the business or subject to  
39 further unauthorized use.

40 (c) "CISO" means the executive branch chief information security  
41 officer.

42 (d) "Cybersecurity"—~~is~~ means the body of information technologies,  
43 processes and practices designed to protect networks, computers, programs

1 and data from attack, damage or unauthorized access.

2 (e) "Cybersecurity positions" do not include information technology  
3 positions within executive branch agencies.

4 (f) "Data in electronic form" means any data stored electronically or  
5 digitally on any computer system or other database and includes  
6 recordable tapes and other mass storage devices.

7 (g) "Executive branch agency" means any agency in the executive  
8 branch of the state of Kansas, *including the judicial council* but ~~does not~~  
9 ~~include~~ *the* elected office agencies, the adjutant general's department, ~~the~~  
10 ~~Kansas public employees retirement system~~, regents' institutions, or the  
11 board of regents.

12 (h) "KISO" means the Kansas information security office.

13 (i) (1) "Personal information" means:

14 (A) An individual's first name or first initial and last name, in  
15 combination with at least one of the following data elements for that  
16 individual:

17 (i) Social security number;

18 (ii) driver's license or identification card number, passport number,  
19 military identification number or other similar number issued on a  
20 government document used to verify identity;

21 (iii) financial account number or credit or debit card number, in  
22 combination with any security code, access code or password that is  
23 necessary to permit access to an individual's financial account;

24 (iv) any information regarding an individual's medical history, mental  
25 or physical condition or medical treatment or diagnosis by a healthcare  
26 professional; or

27 (v) an individual's health insurance policy number or subscriber  
28 identification number and any unique identifier used by a health insurer to  
29 identify the individual; or

30 (B) a user name or email address, in combination with a password or  
31 security question and answer that would permit access to an online  
32 account.

33 (2) "Personal information" does not include information:

34 (A) About an individual that has been made publicly available by a  
35 federal agency, state agency or municipality; or

36 (B) that is encrypted, secured or modified by any other method or  
37 technology that removes elements that personally identify an individual or  
38 that otherwise renders the information unusable.

39 (j) "State agency" means the same as defined in K.S.A. 75-7201, and  
40 amendments thereto.

41 Sec. ~~22~~ {22.} K.S.A. 2023 Supp. 75-7238 is hereby amended to read  
42 as follows: 75-7238. (a) There is hereby established the position of  
43 executive branch chief information security officer (*CISO*). The *executive*

1 CISO shall be in the unclassified service under the Kansas civil service  
2 act, shall be appointed by the governor and shall receive compensation in  
3 an amount fixed by the governor.

4 (b) The *executive* CISO shall:

5 (1) Report to the executive branch chief information technology  
6 officer;

7 (2) ~~serve as the state's CISO;~~

8 ~~(3) serve as the executive branch chief cybersecurity strategist and~~  
9 ~~authority on policies, compliance, procedures, guidance and technologies~~  
10 ~~impacting executive branch cybersecurity programs;~~

11 ~~(4) ensure Kansas information security office resources assigned or~~  
12 ~~provided to executive branch agencies are in compliance with applicable~~  
13 ~~laws and rules and regulations;~~

14 ~~(5) coordinate cybersecurity efforts between executive branch~~  
15 ~~agencies;~~

16 ~~(6) provide guidance to executive branch agencies when compromise~~  
17 ~~of personal information or computer resources has occurred or is likely to~~  
18 ~~occur as the result of an identified high-risk vulnerability or threat;~~

19 ~~(7) set cybersecurity policy and standards for executive branch~~  
20 ~~agencies; and~~

21 ~~(8) perform such other functions and duties as provided by law and as~~  
22 ~~directed by the executive chief information technology officer~~  
23 ~~establish security standards and policies to protect the branch's information~~  
24 ~~technology systems and infrastructure in accordance with subsection (c);~~

25 (3) ensure the confidentiality, availability and integrity of the  
26 information transacted, stored or processed in the branch's information  
27 technology systems and infrastructure;

28 (4) develop a centralized cybersecurity protocol for protecting and  
29 managing executive branch information technology assets and  
30 infrastructure;

31 (5) detect and respond to security incidents consistent with  
32 information security standards and policies;

33 (6) be responsible for the cybersecurity of all executive branch data  
34 and information resources;

35 (7) collaborate with the chief information security officers of the  
36 other branches of state government to respond to cybersecurity incidents;

37 (8) ensure that the governor and all executive branch employees  
38 complete cybersecurity awareness training annually and that if an  
39 employee does not complete the required training such employee's access  
40 to any state-issued hardware or the state network is revoked; and

41 (9) review all contracts related to information technology entered  
42 into by a person or entity within the executive branch to make efforts to  
43 reduce the risk of security vulnerabilities within the supply chain or

1 *product and ensure each contract contains standard security language.*

2 (c) *The executive CISO shall develop a cybersecurity program for*  
 3 *each executive agency that complies with the national institute of*  
 4 *standards and technology cybersecurity framework (CSF) 2.0, as in effect*  
 5 *on July 1, 2024. The executive CISO shall ensure that such programs*  
 6 *achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior*  
 7 *to July 1, 2030. The agency head of each executive agency shall*  
 8 *coordinate with the executive CISO to achieve such standards.*

9 Sec. ~~24~~, {23.} K.S.A. 2023 Supp. 75-7239 is hereby amended to read  
 10 as follows: 75-7239. (a) There is hereby established within and as a part of  
 11 the office of information technology services the Kansas information  
 12 security office. The Kansas information security office shall be  
 13 administered by the *executive* CISO and be staffed appropriately to effect  
 14 the provisions of the Kansas cybersecurity act.

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

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

26 (1) Administer the Kansas cybersecurity act;

27 (2) ~~assist the executive branch in developing, implementing and~~  
 28 ~~monitoring~~ *develop, implement and monitor* strategic and comprehensive  
 29 information security risk-management programs;

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

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

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

39 (6)(4) provide the executive branch strategic risk guidance for  
 40 information technology projects, including the evaluation and  
 41 recommendation of technical controls;

42 (7) ~~assist in the development of executive branch agency~~  
 43 ~~cybersecurity programs to ensure compliance with applicable state and~~

1 federal laws, rules and regulations, executive branch policies and standards  
2 and policies and standards adopted by the information technology  
3 executive council;

4 ~~(8)~~(5) *coordinate with the United States cybersecurity and*  
5 *infrastructure security agency to perform annual audits of executive*  
6 *branch agencies for compliance with applicable state and federal laws,*  
7 *rules and regulations; and executive branch policies and standards—and*  
8 *policies and standards adopted by the information technology executive*  
9 *council. The executive CISO shall make an audit request to such agency*  
10 *annually, regardless of whether or not such agency has the capacity to*  
11 *perform the requested audit;*

12 *(6) perform audits of executive branch agencies for compliance with*  
13 *applicable state and federal laws, rules and regulations, executive branch*  
14 *policies and standards and policies and standards adopted by the*  
15 *information technology executive council;*

16 ~~(9)~~(7) *coordinate the use of external resources involved in*  
17 *information security programs, including, but not limited to, interviewing*  
18 *and negotiating contracts and fees;*

19 ~~(10)~~(8) *liaise with external agencies, such as law enforcement and*  
20 *other advisory bodies as necessary, to ensure a strong security posture;*

21 ~~(11)~~(9) *assist in the development of plans and procedures to manage*  
22 *and recover business-critical services in the event of a cyberattack or other*  
23 *disaster;*

24 ~~(12)~~ *assist executive branch agencies to create a framework for roles*  
25 *and responsibilities relating to information ownership, classification,*  
26 *accountability and protection;*

27 ~~(13)~~(10) *coordinate with executive branch agencies to provide*  
28 *cybersecurity staff to such agencies as necessary;*

29 *(11) ensure a cybersecurity awareness training program is made*  
30 *available to all branches of state government; and*

31 ~~(14)~~(12) *perform such other functions and duties as provided by law*  
32 *and as directed by the CISO.*

33 *(d) (1) If an audit conducted pursuant to subsection (c)(5) results in a*  
34 *failure, the executive CISO shall report such failure to the speaker of the*  
35 *house of representatives and the president of the senate within 30 days of*  
36 *receiving notice of such failure. Such report shall contain a plan to*  
37 *mitigate any security risks identified in the audit. The executive CISO shall*  
38 *coordinate for an additional audit after the mitigation plan is implemented*  
39 *and report the results of such audit to the speaker of the house of*  
40 *representatives and the president of the senate.*

41 *(2) Results of audits conducted pursuant to subsection ~~(c)~~(8) (c)(5)*  
42 *and the reports described in subsection (d)(1) shall be confidential and*  
43 *shall not be subject to discovery or disclosure pursuant to the open records*



1 act, K.S.A. 45-215 et seq., and amendments thereto. ~~The provisions of this~~  
2 ~~subsection shall expire on July 1, 2028, unless the legislature reviews and~~  
3 ~~acts to continue such provision pursuant to K.S.A. 45-229, and~~  
4 ~~amendments thereto, prior to July 1, 2028.~~

5 *(e) There is hereby created in the state treasury the information*  
6 *technology security fund. All expenditures from such fund shall be made in*  
7 *accordance with appropriation acts upon warrants of the director of*  
8 *accounts and reports issued pursuant to vouchers approved by the*  
9 *executive CISO or by a person designated by the executive CISO.*

10 Sec. ~~25~~, {24.} K.S.A. 2023 Supp. 75-7240 is hereby amended to read  
11 as follows: 75-7240. (a) The executive branch agency heads shall:

12 (1) Be ~~solely~~ responsible for security of all data and information  
13 technology resources under such agency's purview, irrespective of the  
14 location of the data or resources. ~~Locations of data may include:~~

15 ~~(A) Agency sites;~~

16 ~~(B) agency real property;~~

17 ~~(C) infrastructure in state data centers;~~

18 ~~(D) third-party locations; and~~

19 ~~(E) in transit between locations;~~

20 ~~(2) ensure that an agency-wide information security program is in~~  
21 ~~place;~~

22 ~~(3)(2) designate an information security officer to administer the~~  
23 ~~agency's information security program that reports directly to executive~~  
24 ~~leadership;~~

25 ~~(4)(3) participate in CISO-sponsored statewide cybersecurity program~~  
26 ~~initiatives and services;~~

27 ~~(5) implement policies and standards to ensure that all the agency's~~  
28 ~~data and information technology resources are maintained in compliance~~  
29 ~~with applicable state and federal laws and rules and regulations;~~

30 ~~(6) implement appropriate cost-effective safeguards to reduce,~~  
31 ~~eliminate or recover from identified threats to data and information~~  
32 ~~technology resources;~~

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

36 ~~(8) (A) submit a cybersecurity self-assessment report to the CISO by~~  
37 ~~October 16 of each even-numbered year, including an executive summary~~  
38 ~~of the findings, that assesses the extent to which the agency is vulnerable~~  
39 ~~to unauthorized access or harm, including the extent to which the agency's~~  
40 ~~or contractor's electronically stored information is vulnerable to alteration,~~  
41 ~~damage, erasure or inappropriate use;~~

42 ~~(B) ensure that the agency conducts annual internal assessments of its~~  
43 ~~security program. Internal assessment results shall be considered~~

1 ~~confidential and shall not be subject to discovery by or release to any~~  
2 ~~person or agency, outside of the KISO or CISO, without authorization~~  
3 ~~from the executive branch agency director or head; and~~

4 ~~(C) prepare or have prepared a financial summary identifying~~  
5 ~~cybersecurity expenditures addressing the findings of the cybersecurity~~  
6 ~~self-assessment report required in subparagraph (A), excluding~~  
7 ~~information that might put the data or information resources of the agency~~  
8 ~~or its contractors at risk and submit such report to the house of~~  
9 ~~representatives committee on appropriations and the senate committee on~~  
10 ~~ways and means; and~~

11 ~~(9)(4) ensure that if an agency owns, licenses or maintains~~  
12 ~~computerized data that includes personal information, confidential~~  
13 ~~information or information, the disclosure of which is regulated by law,~~  
14 ~~such agency shall, in the event of a breach or suspected breach of system~~  
15 ~~security or an unauthorized exposure of that information:~~

16 (A) Comply with the notification requirements set out in K.S.A. 2023  
17 Supp. 50-7a01 et seq., and amendments thereto, and applicable federal  
18 laws and rules and regulations, to the same extent as a person who  
19 conducts business in this state; and

20 (B) not later than ~~48~~ 12 hours after the discovery of the breach,  
21 suspected breach or unauthorized exposure, notify:

22 (i) The CISO; and

23 (ii) if the breach, suspected breach or unauthorized exposure involves  
24 election data, the secretary of state.

25 (b) The director or head of each state agency shall:

26 (1) Participate in annual agency leadership training to ensure  
27 understanding of:

28 (A) The potential impact of common types of cyberattacks and data  
29 breaches on the agency's operations and assets;

30 (B) how cyberattacks and data breaches on the agency's operations  
31 and assets may impact the operations and assets of other governmental  
32 entities on the state enterprise network;

33 (C) how cyberattacks and data breaches occur; and

34 (D) steps to be undertaken by the executive director or agency head  
35 and agency employees to protect their information and information  
36 systems; *and*

37 (2) ~~ensure that all information technology login credentials are~~  
38 ~~disabled the same day that any employee ends their employment with the~~  
39 ~~state; and~~

40 ~~(3) require that all employees with access to information technology~~  
41 ~~receive a minimum of one hour of information technology security~~  
42 ~~training per year coordinate with the executive CISO to implement the~~  
43 ~~security standard described in K.S.A. 75-7238, and amendments thereto.~~

1 (e)(1) ~~The CISO, with input from the joint committee on information~~  
2 ~~technology and the joint committee on Kansas security, shall develop a~~  
3 ~~self-assessment report template for use under subsection (a)(8)(A). The~~  
4 ~~most recent version of such template shall be made available to state~~  
5 ~~agencies prior to July 1 of each even-numbered year. The CISO shall~~  
6 ~~aggregate data from the self-assessments received under subsection (a)(8)~~  
7 ~~(A) and provide a summary of such data to the joint committee on~~  
8 ~~information technology and the joint committee on Kansas security.~~

9 (2) ~~Self-assessment reports made to the CISO pursuant to subsection~~  
10 ~~(a)(8)(A) shall be confidential and shall not be subject to the provisions of~~  
11 ~~the Kansas open records act, K.S.A. 45-215 et seq., and amendments~~  
12 ~~thereto. The provisions of this paragraph shall expire on July 1, 2028,~~  
13 ~~unless the legislature reviews and reenacts this provision pursuant to~~  
14 ~~K.S.A. 45-229, and amendments thereto, prior to July 1, 2028.~~

15 ~~Sec. 26. {25.} K.S.A. 40-110, 75-413, 75-623, 75-710, 75-711 and~~  
16 ~~75-7203 and K.S.A. 2023 Supp. 45-229, 75-7201, 75-7202, 75-7205, 75-~~  
17 ~~7206, 75-7208, 75-7209, 75-7237, 75-7238, 75-7239 and 75-7240 are~~  
18 ~~hereby repealed.~~

19 ~~Sec. 27. {26.} This act shall take effect and be in force from and after~~  
20 ~~its publication in the statute book.~~