

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. Such employees shall be required to
6 use such state-issued information technology hardware to access such
7 applications. The judicial chief information technology officer shall
8 consult with the executive chief information technology officer to develop
9 a plan to allow each piece of information technology hardware that is used
10 to access an application administered by the judicial branch to be part of
11 the KANWIN network prior to July 1, 2027.

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

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

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

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

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

33 (1) Report to the judicial administrator;

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

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

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

42 (5) detect and respond to security incidents consistent with
43 information security standards and policies;

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

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

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

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

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

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

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

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

41 New Sec. 3. (a) There is hereby established the position of legislative
42 branch chief information security officer. The legislative chief information
43 security officer shall be in the unclassified service under the Kansas civil

1 service act, shall be appointed by the legislative coordinating council and
2 shall receive compensation determined by the legislative coordinating
3 council.

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

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

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

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

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

15 (5) detect and respond to security incidents consistent with
16 information security standards and policies;

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

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

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

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

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

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

1 agency head of each legislative agency shall coordinate with the legislative
2 chief information security officer to achieve such standards.

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

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

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

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

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

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

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

43 New Sec. 5.

1 OFFICE OF INFORMATION TECHNOLOGY SERVICES

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

4 Kansas information
5 technology office (335-00-1000).....\$15,000,000

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

26 New Sec. 6.

27 KANSAS INFORMATION SECURITY OFFICE

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

33 Information technology security fund.....No limit

34 New Sec. 7.

35 KANSAS INFORMATION SECURITY OFFICE

36 (a) There is appropriated for the above agency from the following
37 special revenue fund or funds for the fiscal year ending June 30, 2026, all
38 moneys now or hereafter lawfully credited to and available in such fund or
39 funds, except that expenditures other than refunds authorized by law shall
40 not exceed the following:

41 Information technology security fund.....No limit

42 New Sec. 8.

43 ADJUTANT GENERAL

1 (a) There is appropriated for the above agency from the state general
2 fund for the fiscal year ending June 30, 2025, the following:
3 Operating expenditures (034-00-1000-0053).....\$250,000
4 *Provided*, That expenditures shall be made by the above agency from such
5 account for two full-time employees in the Kansas intelligence fusion
6 center to assist in monitoring state information technology systems:
7 *Provided further*, That such employees shall be in the unclassified service
8 of the civil service act and shall be in addition to the positions of the above
9 agency as authorized pursuant to K.S.A. 2023 Supp. 48-3706, and
10 amendments thereto.

11 Sec. 9. K.S.A. 40-110 is hereby amended to read as follows: 40-110.

12 (a) The commissioner of insurance is hereby authorized to appoint an
13 assistant commissioner of insurance, actuaries, two special attorneys who
14 shall have been regularly admitted to practice, an executive secretary,
15 policy examiners, two field representatives, and a secretary to the
16 commissioner. Such appointees shall each receive an annual salary to be
17 determined by the commissioner of insurance, within the limits of
18 available appropriations. The commissioner is also authorized to appoint,
19 within the provisions of the civil service law, and available appropriations,
20 other employees as necessary to administer the provisions of this act. The
21 field representatives authorized by this section may be empowered to
22 conduct inquiries, investigations or to receive complaints. Such field
23 representatives shall not be empowered to make, or direct to be made, an
24 examination of the affairs and financial condition of any insurance
25 company in the process of organization, or applying for admission or
26 doing business in this state.

27 (b) The appointees authorized by this section shall take the proper
28 official oath and shall be in no way interested, except as policyholders, in
29 any insurance company. In the absence of the commissioner of insurance
30 the assistant commissioner shall perform the duties of the commissioner of
31 insurance, but shall in all cases execute papers in the name of the
32 commissioner of insurance, as assistant. The commissioner of insurance
33 shall be responsible for all acts of an official nature done and performed by
34 the commissioner's assistant or any person employed in such office. All the
35 appointees authorized by this section shall hold their office at the will and
36 pleasure of the commissioner of insurance.

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

41 (1) *Develop a cybersecurity program for the department that*
42 *complies with the national institute of standards and technology*
43 *cybersecurity framework (CSF) 2.0, as in effect on July 1, 2024. The chief*

1 *information security officer shall ensure that such programs achieve a*
2 *CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior to July 1,*
3 *2030;*

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

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

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

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

18 Sec. 10. K.S.A. 2023 Supp. 45-229 is hereby amended to read as
19 follows: 45-229. (a) It is the intent of the legislature that exceptions to
20 disclosure under the open records act shall be created or maintained only
21 if:

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

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

26 (3) the public record affects confidential information.

27 The maintenance or creation of an exception to disclosure must be
28 compelled as measured by these criteria. Further, the legislature finds that
29 the public has a right to have access to public records unless the criteria in
30 this section for restricting such access to a public record are met and the
31 criteria are considered during legislative review in connection with the
32 particular exception to disclosure to be significant enough to override the
33 strong public policy of open government. To strengthen the policy of open
34 government, the legislature shall consider the criteria in this section before
35 enacting an exception to disclosure.

36 (b) Subject to the provisions of subsections (g) and (h), any new
37 exception to disclosure or substantial amendment of an existing exception
38 shall expire on July 1 of the fifth year after enactment of the new
39 exception or substantial amendment, unless the legislature acts to continue
40 the exception. A law that enacts a new exception or substantially amends
41 an existing exception shall state that the exception expires at the end of
42 five years and that the exception shall be reviewed by the legislature
43 before the scheduled date.

1 (c) For purposes of this section, an exception is substantially
2 amended if the amendment expands the scope of the exception to include
3 more records or information. An exception is not substantially amended if
4 the amendment narrows the scope of the exception.

5 (d) This section is not intended to repeal an exception that has been
6 amended following legislative review before the scheduled repeal of the
7 exception if the exception is not substantially amended as a result of the
8 review.

9 (e) In the year before the expiration of an exception, the revisor of
10 statutes shall certify to the president of the senate and the speaker of the
11 house of representatives, by July 15, the language and statutory citation of
12 each exception that will expire in the following year that meets the criteria
13 of an exception as defined in this section. Any exception that is not
14 identified and certified to the president of the senate and the speaker of the
15 house of representatives is not subject to legislative review and shall not
16 expire. If the revisor of statutes fails to certify an exception that the revisor
17 subsequently determines should have been certified, the revisor shall
18 include the exception in the following year's certification after that
19 determination.

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

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

27 (1) Is required by federal law;
28 (2) applies solely to the legislature or to the state court system;
29 (3) has been reviewed and continued in existence twice by the
30 legislature; ~~or~~

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

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

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

37 (A) What specific records are affected by the exception;
38 (B) whom does the exception uniquely affect, as opposed to the
39 general public;

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

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

43 (2) an exception may be created or maintained only if it serves an

1 identifiable public purpose and may be no broader than is necessary to
2 meet the public purpose it serves. An identifiable public purpose is served
3 if the legislature finds that the purpose is sufficiently compelling to
4 override the strong public policy of open government and cannot be
5 accomplished without the exception and if the exception:

6 (A) Allows the effective and efficient administration of a
7 governmental program that would be significantly impaired without the
8 exception;

9 (B) protects information of a sensitive personal nature concerning
10 individuals, the release of such information would be defamatory to such
11 individuals or cause unwarranted damage to the good name or reputation
12 of such individuals or would jeopardize the safety of such individuals.
13 Only information that would identify the individuals may be excepted
14 under this paragraph; or

15 (C) protects information of a confidential nature concerning entities,
16 including, but not limited to, a formula, pattern, device, combination of
17 devices, or compilation of information that is used to protect or further a
18 business advantage over those who do not know or use it, if the disclosure
19 of such information would injure the affected entity in the marketplace.

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

26 (i) (1) Exceptions contained in the following statutes as continued in
27 existence in section 2 of chapter 126 of the 2005 Session Laws of Kansas
28 and that have been reviewed and continued in existence twice by the
29 legislature as provided in subsection (g) are hereby continued in existence:
30 1-401, 2-1202, 5-512, 9-1137, 9-1712, 9-2217, 10-630, 12-189, 12-1,108,
31 12-1694, 12-1698, 12-2819, 12-4516, 16-715, 16a-2-304, 17-1312e, 17-
32 2227, 17-5832, 17-7511, 17-76,139, 19-4321, 21-2511, 22-3711, 22-4707,
33 22-4909, 22a-243, 22a-244, 23-605, 23-9,312, 25-4161, 25-4165, 31-405,
34 34-251, 38-2212, 39-709b, 39-719e, 39-934, 39-1434, 39-1704, 40-222,
35 40-2,156, 40-2c20, 40-2c21, 40-2d20, 40-2d21, 40-409, 40-956, 40-1128,
36 40-2807, 40-3012, 40-3304, 40-3308, 40-3403b, 40-3421, 40-3613, 40-
37 3805, 40-4205, 44-510j, 44-550b, 44-594, 44-635, 44-714, 44-817, 44-
38 1005, 44-1019, 45-221(a)(1) through (43), 46-256, 46-259, 46-2201, 47-
39 839, 47-844, 47-849, 47-1709, 48-1614, 49-406, 49-427, 55-1,102, 58-
40 4114, 59-2135, 59-2802, 59-2979, 59-29b79, 60-3333, 60-3336, 65-102b,
41 65-118, 65-119, 65-153f, 65-170g, 65-177, 65-1,106, 65-1,113, 65-1,116,
42 65-1,157a, 65-1,163, 65-1,165, 65-1,168, 65-1,169, 65-1,171, 65-1,172,
43 65-436, 65-445, 65-507, 65-525, 65-531, 65-657, 65-1135, 65-1467, 65-

1 1627, 65-1831, 65-2422d, 65-2438, 65-2836, 65-2839a, 65-2898a, 65-
2 3015, 65-3447, 65-34,108, 65-34,126, 65-4019, 65-4922, 65-4925, 65-
3 5602, 65-5603, 65-6002, 65-6003, 65-6004, 65-6010, 65-67a05, 65-6803,
4 65-6804, 66-101c, 66-117, 66-151, 66-1,190, 66-1,203, 66-1220a, 66-
5 2010, 72-2232, 72-3438, 72-6116, 72-6267, 72-9934, 73-1228, 74-2424,
6 74-2433f, 74-32,419, 74-4905, 74-4909, 74-50,131, 74-5515, 74-7308, 74-
7 7338, 74-8104, 74-8307, 74-8705, 74-8804, 74-9805, 75-104, 75-712, 75-
8 7b15, 75-1267, 75-2943, 75-4332, 75-4362, 75-5133, 75-5266, 75-5665,
9 75-5666, 75-7310, 76-355, 76-359, 76-493, 76-12b11, 76-12c03, 76-3305,
10 79-1119, 79-1437f, 79-3234, 79-3395, 79-3420, 79-3499, 79-34,113, 79-
11 3614, 79-3657, 79-4301 and 79-5206.

12 (2) Exceptions contained in the following statutes as certified by the
13 revisor of statutes to the president of the senate and the speaker of the
14 house of representatives pursuant to subsection (e) and that have been
15 reviewed during the 2015 legislative session and continued in existence by
16 the legislature as provided in subsection (g) are hereby continued in
17 existence: 17-2036, 40-5301, 45-221(a)(45), (46) and (49), 48-16a10, 58-
18 4616, 60-3351, 72-3415, 74-50,217 and 75-53,105.

19 (j) (1) Exceptions contained in the following statutes as continued in
20 existence in section 1 of chapter 87 of the 2006 Session Laws of Kansas
21 and that have been reviewed and continued in existence twice by the
22 legislature as provided in subsection (g) are hereby continued in existence:
23 1-501, 9-1303, 12-4516a, 39-970, 65-525, 65-5117, 65-6016, 65-6017 and
24 74-7508.

25 (2) 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 2015 and that
28 have been reviewed during the 2016 legislative session are hereby
29 continued in existence: 12-5611, 22-4906, 22-4909, 38-2310, 38-2311, 38-
30 2326, 40-955, 44-1132, 45-221(a)(10)(F) and (a)(50), 60-3333, 65-4a05,
31 65-445(g), 65-6154, 71-218, 75-457, 75-712c, 75-723 and 75-7c06.

32 (k) 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) and that have been
35 reviewed during the 2014 legislative session and continued in existence by
36 the legislature as provided in subsection (g) are hereby continued in
37 existence: 1-205, 2-2204, 8-240, 8-247, 8-255c, 8-1324, 8-1325, 12-
38 17,150, 12-2001, 17-12a607, 38-1008, 38-2209, 40-5006, 40-5108, 41-
39 2905, 41-2906, 44-706, 44-1518, 45-221(a)(44), (45), (46), (47) and (48),
40 50-6a11, 65-1,243, 65-16,104, 65-3239, 74-50,184, 74-8134, 74-99b06,
41 77-503a and 82a-2210.

42 (l) Exceptions contained in the following statutes as certified by the
43 revisor of statutes to the president of the senate and the speaker of the

1 house of representatives pursuant to subsection (e) during 2016 and that
2 have been reviewed during the 2017 legislative session are hereby
3 continued in existence: 12-5711, 21-2511, 22-4909, 38-2313, 45-221(a)
4 (51) and (52), 65-516, 65-1505, 74-2012, 74-5607, 74-8745, 74-8752, 74-
5 8772, 75-7d01, 75-7d05, 75-5133, 75-7427 and 79-3234.

6 (m) Exceptions contained in the following statutes as certified by the
7 revisor of statutes to the president of the senate and the speaker of the
8 house of representatives pursuant to subsection (e) during 2012 and that
9 have been reviewed during the 2013 legislative session and continued in
10 existence by the legislature as provided in subsection (g) are hereby
11 continued in existence: 12-5811, 40-222, 40-223j, 40-5007a, 40-5009a,
12 40-5012a, 65-1685, 65-1695, 65-2838a, 66-1251, 66-1805, 72-8268, 75-
13 712 and 75-5366.

14 (n) Exceptions contained in the following statutes as certified by the
15 revisor of statutes to the president of the senate and the speaker of the
16 house of representatives pursuant to subsection (e) and that have been
17 reviewed during the 2018 legislative session are hereby continued in
18 existence: 9-513c(c)(2), 39-709, 45-221(a)(26), (53) and (54), 65-6832,
19 65-6834, 75-7c06 and 75-7c20.

20 (o) Exceptions contained in the following statutes as certified by the
21 revisor of statutes to the president of the senate and the speaker of the
22 house of representatives pursuant to subsection (e) that have been
23 reviewed during the 2019 legislative session are hereby continued in
24 existence: 21-2511(h)(2), 21-5905(a)(7), 22-2302(b) and (c), 22-2502(d)
25 and (e), 40-222(k)(7), 44-714(e), 45-221(a)(55), 46-1106(g) regarding 46-
26 1106(i), 65-2836(i), 65-2839a(c), 65-2842(d), 65-28a05(n), article 6(d) of
27 65-6230, 72-6314(a) and 74-7047(b).

28 (p) Exceptions contained in the following statutes as certified by the
29 revisor of statutes to the president of the senate and the speaker of the
30 house of representatives pursuant to subsection (e) that have been
31 reviewed during the 2020 legislative session are hereby continued in
32 existence: 38-2310(c), 40-409(j)(2), 40-6007(a), 45-221(a)(52), 46-1129,
33 59-29a22(b)(10) and 65-6747.

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

40 (r) 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) that have been
43 reviewed during the 2023 legislative session are hereby continued in

1 existence: 2-3902 and 66-2020.

2 Sec. 11. K.S.A. 75-413 is hereby amended to read as follows: 75-413.

3 (a) The secretary of state may appoint such other assistants and clerks as
4 may be authorized by law; but the secretary of state shall be responsible
5 for the proper discharge of the duties of all assistants and clerks, and they
6 shall hold their offices at the will and pleasure of the secretary and shall do
7 and perform such general duties as the secretary may require.

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

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

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

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

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

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

31 Sec. 12. K.S.A. 75-623 is hereby amended to read as follows: 75-623.

32 (a) The treasurer shall appoint such other assistants, clerks, bookkeepers,
33 accountants and stenographers as may be authorized by law, each of which
34 persons shall take the oath of office required of public officers. Such
35 persons shall hold their offices at the will and pleasure of the state
36 treasurer.

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

41 (1) *Develop a cybersecurity program for the office that complies with*
42 *the national institute of standards and technology cybersecurity*
43 *framework (CSF) 2.0, as in effect on July 1, 2024. The 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;*

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

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

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

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

17 Sec. 13. K.S.A. 75-710 is hereby amended to read as follows: 75-710.

18 (a) The attorney general shall appoint such assistants, clerks, and
19 stenographers as shall be authorized by law, and who shall hold their office
20 at the will and pleasure of the attorney general. All fees and allowances
21 earned by said assistants or any of them, or allowed to them by any statute
22 or order of court in any civil or criminal case whatsoever, shall be turned
23 into the general revenue fund of the state treasury, and the vouchers for
24 their monthly salaries shall not be honored by the director of accounts and
25 reports until a verified account of the fees collected by them, or either of
26 them, during the preceding month, has been filed in the director of
27 accounts and reports' office. Assistants appointed by the attorney general
28 shall perform the duties and exercise the powers as prescribed by law and
29 shall perform other duties as prescribed by the attorney general. Assistants
30 shall act for and exercise the power of the attorney general to the extent
31 the attorney general delegates them the authority to do so.

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

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

41 (2) *ensure that the attorney general and all employees complete*
42 *cybersecurity awareness training annually and that if an employee does*
43 *not complete the required training, such employee's access to any state-*

1 *issued hardware or the state network is revoked; and*

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

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

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

12 Sec. 14. K.S.A. 75-711 is hereby amended to read as follows: 75-711.

13 (a) There is hereby established, under the jurisdiction of the attorney
14 general, a division to be known as the Kansas bureau of investigation. The
15 director of the bureau shall be appointed by the attorney general, subject to
16 confirmation by the senate as provided in K.S.A. 75-4315b, and
17 amendments thereto, and shall have special training and qualifications for
18 such position. Except as provided by K.S.A. 46-2601, and amendments
19 thereto, no person appointed as director shall exercise any power, duty or
20 function as director until confirmed by the senate. In accordance with
21 appropriation acts, the director shall appoint agents who shall be trained in
22 the detection and apprehension of criminals. The director shall appoint an
23 associate director, and any such assistant directors from within the agency
24 as are necessary for the efficient operation of the bureau, who shall have
25 the qualifications and employee benefits, including longevity, of an agent.
26 The director also may appoint a deputy director and, in accordance with
27 appropriation acts, such administrative employees as are necessary for the
28 efficient operation of the bureau. No person shall be appointed to a
29 position within the Kansas bureau of investigation if the person has been
30 convicted of a felony.

31 (b) The director, associate director, deputy director, assistant directors
32 and any assistant attorneys general assigned to the bureau shall be within
33 the unclassified service under the Kansas civil service act. All other agents
34 and employees of the bureau shall be in the classified service under the
35 Kansas civil service act and their compensation shall be determined as
36 provided in the Kansas civil service act and shall receive actual and
37 necessary expenses.

38 (c) Any person who was a member of the bureau at the time of
39 appointment as director, associate director or assistant director, upon the
40 expiration of their appointment, shall be returned to an unclassified or
41 regular classified position under the Kansas civil service act with
42 compensation comparable to and not lower than compensation being
43 received at the time of appointment to the unclassified service. If all such

1 possible positions are filled at that time, a temporary additional position
2 shall be created for the person until a vacancy exists in the position. While
3 serving in the temporary additional position, the person shall continue to
4 be a contributing member of the retirement system for the agents of the
5 Kansas bureau of investigation.

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

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

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

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

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

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

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

32 Sec. 15. K.S.A. 2023 Supp. 75-7201 is hereby amended to read as
33 follows: 75-7201. As used in K.S.A. 75-7201 through 75-7212, and
34 amendments thereto:

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

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

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

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

8 (e) "Information technology project change or overrun" means any
9 change in:

10 (1) Planned expenditures for an information technology project that
11 would result in the total authorized cost of the project being increased
12 above the currently authorized cost of such project by more than 10% of
13 such currently authorized cost of such project or an established threshold
14 within the information technology executive council's policies *or policies*
15 *adopted by the judicial branch or the legislative coordinating council;*

16 (2) the scope or project timeline of an information technology project,
17 as such scope or timeline was presented to and reviewed by the joint
18 committee or the chief information technology officer to whom the project
19 was submitted pursuant to K.S.A. 75-7209, and amendments thereto, that
20 is a change of more than 10% or a change that is significant as determined
21 by the information technology executive council's policies *or policies*
22 *adopted by the judicial branch or the legislative coordinating council;* or

23 (3) the proposed use of any new or replacement information
24 technology equipment or in the use of any existing information technology
25 equipment that has been significantly upgraded.

26 (f) "Joint committee" means the joint committee on information
27 technology.

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

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

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

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

41 (k) "Project start" means the date and time when a state agency
42 begins a formal study of a business process or technology concept to
43 assess the needs of the state agency, determines project feasibility or

1 prepares an information technology project budget estimate under K.S.A.
2 75-7209, and amendments thereto.

3 (l) "State agency" means any state office or officer, department,
4 board, commission, institution or bureau, or any agency, division or unit
5 thereof.

6 Sec. 16. K.S.A. 2023 Supp. 75-7202 is hereby amended to read as
7 follows: 75-7202. (a) There is hereby established the information
8 technology executive council which shall be attached to the office of
9 information technology services for purposes of administrative functions.

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

12 (A) Two cabinet agency heads or such persons' designees;

13 (B) two noncabinet agency heads or such persons' designees;

14 (C) the executive chief information technology officer;

15 (D) ~~the legislative chief information technology officer;~~

16 ~~(E) the judicial chief information technology officer;~~

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

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

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

22 ~~(I)~~(G) one representative with background and knowledge in
23 technology and cybersecurity from the private sector, except that such
24 representative or such representative's employer shall not be an
25 information technology or cybersecurity vendor that does business with
26 the state of Kansas;

27 ~~(J)~~(H) one representative appointed by the Kansas criminal justice
28 information system committee; *and*

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

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

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

35 ~~(N) one member of the house of representatives appointed by the~~
36 ~~minority leader of the house of representatives or such member's~~
37 ~~designee~~(I) *two information technology employees from state board of*

38 *regents institutions appointed by the board of regents.*

39 (2) The chief information technology architect, *the legislative chief*
40 *information technology officer, the judicial chief information technology*
41 *officer, one member of the senate appointed by the president of the senate,*
42 *one member of the senate appointed by the minority leader of the senate,*
43 *one member of the house of representatives appointed by the speaker of*

1 *the house of representatives and one member of the house of*
2 *representatives appointed by the minority leader of the house of*
3 *representatives shall be a nonvoting member nonvoting members of the*
4 *council.*

5 (3) The cabinet agency heads, the noncabinet agency heads, the
6 representative of cities, the representative of counties and the
7 representative from the private sector shall be appointed by the governor
8 for a term not to exceed 18 months. Upon expiration of an appointed
9 member's term, the member shall continue to hold office until the
10 appointment of a successor. Legislative members shall remain members of
11 the legislature in order to retain membership on the council and shall serve
12 until replaced pursuant to this section. Vacancies of members during a term
13 shall be filled in the same manner as the original appointment only for the
14 unexpired part of the term. The appointing authority for a member may
15 remove the member, reappoint the member or substitute another appointee
16 for the member at any time. Nonappointed members shall serve *ex officio*.

17 (c) The chairperson of the council shall be ~~drawn from the chief~~
18 ~~information technology officers, with each chief information technology~~
19 ~~officer serving a one-year term. The term of chairperson shall rotate~~
20 ~~among the chief information technology officers on an annual basis~~ *the*
21 *executive chief information technology officer.*

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

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

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

35 Sec. 17. K.S.A. 75-7203 is hereby amended to read as follows: 75-
36 7203. (a) The information technology executive council is hereby
37 authorized to adopt such policies and rules and regulations as necessary to
38 implement, administer and enforce the provisions of this act.

39 (b) The council shall:

40 (1) Adopt:

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

43 (B) an information technology architecture, including

1 telecommunications systems, networks and equipment, that covers all state
2 agencies;

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

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

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

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

13 (4) *develop a plan to integrate all information technology services*
14 *for the executive branch into the office of information technology services;*
15 *and*

16 (5) perform such other functions and duties as necessary to carry out
17 the provisions of this act.

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

23 Sec. 18. K.S.A. 2023 Supp. 75-7205 is hereby amended to read as
24 follows: 75-7205. (a) There is hereby established within and as a part of
25 the office of information technology services the position of executive
26 chief information technology officer. The executive chief information
27 technology officer shall be in the unclassified service under the Kansas
28 civil service act, shall be appointed by the governor, and shall receive
29 compensation in an amount fixed by the governor. The executive chief
30 information technology officer shall maintain a presence in any cabinet
31 established by the governor and shall report to the governor.

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

33 (1) Review and consult with each executive agency regarding
34 information technology plans, deviations from the state information
35 technology architecture, information technology project estimates and
36 information technology project changes and overruns submitted by such
37 agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine
38 whether the agency has complied with:

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

42 (B) the information technology architecture adopted by the
43 information technology executive council;

- 1 (C) the standards for data management adopted by the information
2 technology executive council; and
- 3 (D) the strategic information technology management plan adopted
4 by the information technology executive council;
- 5 (2) report to the chief information technology architect all deviations
6 from the state information architecture that are reported to the executive
7 information technology officer by executive agencies;
- 8 (3) submit recommendations to the division of the budget as to the
9 technical and management merit of information technology projects and
10 information technology project changes and overruns submitted by
11 executive agencies that are reportable pursuant to K.S.A. 75-7209, and
12 amendments thereto;
- 13 (4) monitor executive agencies' compliance with:
- 14 (A) The information technology resource policies and procedures and
15 project management methodologies adopted by the information technology
16 executive council;
- 17 (B) the information technology architecture adopted by the
18 information technology executive council;
- 19 (C) the standards for data management adopted by the information
20 technology executive council; and
- 21 (D) the strategic information technology management plan adopted
22 by the information technology executive council;
- 23 (5) coordinate implementation of new information technology among
24 executive agencies and with the judicial and legislative chief information
25 technology officers;
- 26 (6) designate the ownership of information resource processes and the
27 lead agency for implementation of new technologies and networks shared
28 by multiple agencies within the executive branch of state government; ~~and~~
- 29 (7) perform such other functions and duties as provided by law or as
30 directed by the governor;
- 31 (8) *consult with the appropriate legal counsel on topics related to*
32 *confidentiality of information, the open records act, K.S.A. 45-215 et seq.,*
33 *and amendments thereto, the open meetings act, K.S.A. 75-4317 et seq.,*
34 *and amendments thereto, and any other legal matter related to*
35 *information technology;*
- 36 (9) *ensure that each executive agency has the necessary information*
37 *technology and cybersecurity staff imbedded within the agency to*
38 *accomplish the agency's duties;*
- 39 (10) *maintain all third-party data centers at locations within the*
40 *United States or with companies that are based in the United States; and*
- 41 (11) *create a database of all electronic devices within the branch and*
42 *ensure that each device is inventoried, cataloged and tagged within an*
43 *inventory device.*

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

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

13 Sec. 19. K.S.A. 2023 Supp. 75-7206 is hereby amended to read as
14 follows: 75-7206. (a) There is hereby established within and as a part of
15 the office of the state judicial administrator the position of judicial chief
16 information technology officer. The judicial chief information technology
17 officer shall be appointed by the judicial administrator, subject to approval
18 of the chief justice, and shall receive compensation determined by the
19 judicial administrator, subject to approval of the chief justice.

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

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

27 ~~(A) The information technology resource policies and procedures and~~
28 ~~project management methodologies adopted by the information technology~~
29 ~~executive council;~~

30 ~~(B) the information technology architecture adopted by the~~
31 ~~information technology executive council;~~

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

34 ~~(D) the strategic information technology management plan adopted~~
35 ~~by the information technology executive council policies and procedures~~
36 ~~adopted by the judicial branch;~~

37 (2) report to the chief information technology architect all deviations
38 from the state information architecture that are reported to the judicial
39 information technology officer by judicial agencies;

40 (3) submit recommendations to the judicial administrator as to the
41 technical and management merit of information technology projects and
42 information technology project changes and overruns submitted by judicial
43 agencies that are reportable pursuant to K.S.A. 75-7209, and amendments

1 thereto;

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

3 ~~(A) The information technology resource policies and procedures and~~
4 ~~project management methodologies adopted by the information technology~~
5 ~~executive council;~~

6 ~~(B) the information technology architecture adopted by the~~
7 ~~information technology executive council;~~

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

10 ~~(D) the strategic information technology management plan adopted~~
11 ~~by the information technology executive council;~~

12 ~~(5)(4) coordinate implementation of new information technology~~
13 ~~among judicial agencies and with the executive and legislative chief~~
14 ~~information technology officers;~~

15 ~~(6)(5) designate the ownership of information resource processes and~~
16 ~~the lead agency for implementation of new technologies and networks~~
17 ~~shared by multiple agencies within the judicial branch of state~~
18 ~~government; and~~

19 ~~(7)(6) perform such other functions and duties as provided by law or~~
20 ~~as directed by the judicial administrator;~~

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

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

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

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

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

41 Sec. 20. K.S.A. 2023 Supp. 75-7208 is hereby amended to read as
42 follows: 75-7208. (a) The legislative chief information technology officer
43 shall:

- 1 (a)(1) Review and consult with each legislative agency regarding
2 information technology plans, deviations from the state information
3 technology architecture, information technology project estimates and
4 information technology project changes and overruns submitted by such
5 agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine
6 whether the agency has complied with the:
- 7 ~~(1) Information technology resource policies and procedures and~~
8 ~~project management methodologies adopted by the information technology~~
9 ~~executive council;~~
- 10 ~~(2) information technology architecture adopted by the information~~
11 ~~technology executive council;~~
- 12 ~~(3) standards for data management adopted by the information~~
13 ~~technology executive council; and~~
- 14 ~~(4) strategic information technology management plan adopted by the~~
15 ~~information technology executive council~~ *policies and procedures adopted*
16 *by the legislative coordinating council;*
- 17 (b)(2) report to the chief information technology architect all
18 deviations from the state information architecture that are reported to the
19 legislative information technology officer by legislative agencies;
- 20 (c)(3) submit recommendations to the legislative coordinating council
21 as to the technical and management merit of information technology
22 projects and information technology project changes and overruns
23 submitted by legislative agencies that are reportable pursuant to K.S.A. 75-
24 7209, and amendments thereto;
- 25 ~~(d) monitor legislative agencies' compliance with the:~~
- 26 ~~(1) Information technology resource policies and procedures and~~
27 ~~project management methodologies adopted by the information technology~~
28 ~~executive council;~~
- 29 ~~(2) information technology architecture adopted by the information~~
30 ~~technology executive council;~~
- 31 ~~(3) standards for data management adopted by the information~~
32 ~~technology executive council; and~~
- 33 ~~(4) strategic information technology management plan adopted by the~~
34 ~~information technology executive council;~~
- 35 (c)(4) coordinate implementation of new information technology
36 among legislative agencies and with the executive and judicial chief
37 information technology officers;
- 38 (f)(5) designate the ownership of information resource processes and
39 the lead agency for implementation of new technologies and networks
40 shared by multiple agencies within the legislative branch of state
41 government;
- 42 ~~(g)(6) serve as staff of the joint committee; and~~
- 43 (h)(7) perform such other functions and duties as provided by law or

1 as directed by the legislative coordinating council or the joint committee;

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

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

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

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

15 (12) *set standards for the legislative division of post audit to use*
16 *when conducting information technology audits that are subject to*
17 *approval by the legislative coordinating council.*

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

22 (c) *The legislative chief information technology officer may make a*
23 *request to the adjutant general to permit the Kansas national guard in a*
24 *state active duty capacity to perform vulnerability assessments or other*
25 *assessments of the branch for the purpose of enhancing security. During*
26 *such vulnerability assessments, members performing the assessment shall,*
27 *to the extent possible, ensure that no harm is done to the systems being*
28 *assessed. The legislative chief information technology officer shall notify*
29 *the legislative agency that owns the information systems being assessed*
30 *about such assesment and coordinate to mitigate the security risk.*

31 Sec. 21. K.S.A. 2023 Supp. 75-7209 is hereby amended to read as
32 follows: 75-7209. (a) (1) Whenever an agency proposes an information
33 technology project, such agency shall prepare and submit information
34 technology project documentation to the chief information technology
35 officer of the branch of state government of which the agency is a part.
36 Such information technology project documentation shall:

37 (A) Include a financial plan showing the proposed source of funding
38 and categorized expenditures for each phase of the project and cost
39 estimates for any needs analyses or other investigations, consulting or
40 other professional services, computer programs, data, equipment, buildings
41 or major repairs or improvements to buildings and other items or services
42 necessary for the project; and

43 (B) be consistent with:

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

3 (ii) an information technology architecture, including
4 telecommunications systems, networks and equipment, that covers all state
5 agencies;

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

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

8 (2) Any information technology project with significant business risk,
9 as determined pursuant to the information technology executive council's
10 policies *or policies adopted by the judicial branch or the legislative*
11 *coordinating council*, shall be presented to the joint committee on
12 information technology by such branch chief information technology
13 officer.

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

16 (A) Specifications for bids or proposals for such project shall be
17 submitted to the chief information technology officer of the branch of state
18 government of which the agency or agencies are a part. Information
19 technology projects requiring chief information technology officer
20 approval shall also require the chief information technology officer's
21 written approval on specifications for bids or proposals; and

22 (B) (i) The chief information technology officer of the appropriate
23 branch over the state agency or agencies that are involved in such project
24 shall submit the project, the project plan, including the architecture, and
25 the cost-benefit analysis to the joint committee on information technology
26 to advise and consult on the project. Such chief information technology
27 officer shall submit such information to each member of the joint
28 committee and to the director of the legislative research department. Each
29 such project plan summary shall include a notice specifying the date the
30 summary was mailed or emailed. After receiving any such project plan
31 summary, each member shall review the information and may submit
32 questions, requests for additional information or request a presentation and
33 review of the proposed project at a meeting of the joint committee. If two
34 or more members of the joint committee contact the director of the
35 legislative research department within seven business days of the date
36 specified in the summary description and request that the joint committee
37 schedule a meeting for such presentation and review, then the director of
38 the legislative research department shall notify the chief information
39 technology officer of the appropriate branch, the head of such agency and
40 the chairperson of the joint committee that a meeting has been requested
41 for such presentation and review on the next business day following the
42 members' contact with the director of the legislative research department.
43 Upon receiving such notification, the chairperson shall call a meeting of

1 the joint committee as soon as practicable for the purpose of such
2 presentation and review and shall furnish the chief information technology
3 officer of the appropriate branch and the head of such agency with notice
4 of the time, date and place of the meeting. Except as provided in
5 subsection (b)(1)(B)(ii), the state agency shall not authorize or approve the
6 release of any request for proposal or other bid event for an information
7 technology project without having first advised and consulted with the
8 joint committee at a meeting.

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

14 (a) Fewer than two members of the joint committee contact the
15 director of the legislative research department within seven business days
16 of the date the project plan summary was mailed and request a committee
17 meeting for a presentation and review of any such proposed request for
18 proposal or other bid event for an information technology project; or

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

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

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

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

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

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

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

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

3 Sec. 22. K.S.A. 2023 Supp. 75-7237 is hereby amended to read as
4 follows: 75-7237. As used in K.S.A. 75-7236 through 75-7243, and
5 amendments thereto:

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

7 (b) "Breach" or "breach of security" means unauthorized access of
8 data in electronic form containing personal information. Good faith access
9 of personal information by an employee or agent of an executive branch
10 agency does not constitute a breach of security, provided that the
11 information is not used for a purpose unrelated to the business or subject to
12 further unauthorized use.

13 (c) "CISO" means the executive branch chief information security
14 officer.

15 (d) "Cybersecurity"~~is~~ means the body of information technologies,
16 processes and practices designed to protect networks, computers, programs
17 and data from attack, damage or unauthorized access.

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

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

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

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

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

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

33 (i) Social security number;

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

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

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

43 (v) an individual's health insurance policy number or subscriber

1 identification number and any unique identifier used by a health insurer to
2 identify the individual; or

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

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

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

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

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

14 Sec. 23. K.S.A. 2023 Supp. 75-7238 is hereby amended to read as
15 follows: 75-7238. (a) There is hereby established the position of executive
16 branch chief information security officer (*CISO*). The *executive* CISO shall
17 be in the unclassified service under the Kansas civil service act, shall be
18 appointed by the governor and shall receive compensation in an amount
19 fixed by the governor.

20 (b) The *executive* CISO shall:

21 (1) Report to the executive branch chief information technology
22 officer;

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

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

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

30 ~~(5) coordinate cybersecurity efforts between executive branch~~
31 ~~agencies;~~

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

35 ~~(7) set cybersecurity policy and standards for executive branch~~
36 ~~agencies; and~~

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

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

1 (4) develop a centralized cybersecurity protocol for protecting and
2 managing executive branch information technology assets and
3 infrastructure;

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

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

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

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

14 (9) review all contracts related to information technology entered
15 into by a person or entity within the executive branch to make efforts to
16 reduce the risk of security vulnerabilities within the supply chain or
17 product and ensure each contract contains standard security language.

18 (c) The executive CISO shall develop a cybersecurity program for
19 each executive agency that complies with the national institute of
20 standards and technology cybersecurity framework (CSF) 2.0, as in effect
21 on July 1, 2024. The executive CISO shall ensure that such programs
22 achieve a CSF tier of 3.0 prior to July 1, 2028, and a CSF tier of 4.0 prior
23 to July 1, 2030. The agency head of each executive agency shall
24 coordinate with the executive CISO to achieve such standards.

25 Sec. 24. K.S.A. 2023 Supp. 75-7239 is hereby amended to read as
26 follows: 75-7239. (a) There is hereby established within and as a part of
27 the office of information technology services the Kansas information
28 security office. The Kansas information security office shall be
29 administered by the *executive* CISO and be staffed appropriately to effect
30 the provisions of the Kansas cybersecurity act.

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

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

42 (1) Administer the Kansas cybersecurity act;

43 (2) ~~assist the executive branch in developing, implementing and~~

1 ~~monitoring~~ *develop, implement and monitor* strategic and comprehensive
 2 information security risk-management programs;

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

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

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

12 ~~(6)(4) provide the executive branch strategic risk guidance for~~
 13 ~~information technology projects, including the evaluation and~~
 14 ~~recommendation of technical controls;~~

15 ~~(7) assist in the development of executive branch agency~~
 16 ~~cybersecurity programs to ensure compliance with applicable state and~~
 17 ~~federal laws, rules and regulations, executive branch policies and standards~~
 18 ~~and policies and standards adopted by the information technology~~
 19 ~~executive council;~~

20 ~~(8)(5) coordinate with the United States cybersecurity and~~
 21 ~~infrastructure security agency to perform annual audits of executive~~
 22 ~~branch agencies for compliance with applicable state and federal laws,~~
 23 ~~rules and regulations; and executive branch policies and standards and~~
 24 ~~policies and standards adopted by the information technology executive~~
 25 ~~council. The executive CISO shall make an audit request to such agency~~
 26 ~~annually, regardless of whether or not such agency has the capacity to~~
 27 ~~perform the requested audit;~~

28 ~~(6) perform audits of executive branch agencies for compliance with~~
 29 ~~applicable state and federal laws, rules and regulations, executive branch~~
 30 ~~policies and standards and policies and standards adopted by the~~
 31 ~~information technology executive council;~~

32 ~~(9)(7) coordinate the use of external resources involved in~~
 33 ~~information security programs, including, but not limited to, interviewing~~
 34 ~~and negotiating contracts and fees;~~

35 ~~(10)(8) liaise with external agencies, such as law enforcement and~~
 36 ~~other advisory bodies as necessary, to ensure a strong security posture;~~

37 ~~(11)(9) assist in the development of plans and procedures to manage~~
 38 ~~and recover business-critical services in the event of a cyberattack or other~~
 39 ~~disaster;~~

40 ~~(12) assist executive branch agencies to create a framework for roles~~
 41 ~~and responsibilities relating to information ownership, classification,~~
 42 ~~accountability and protection;~~

43 ~~(13)(10) coordinate with executive branch agencies to provide~~

1 *cybersecurity staff to such agencies as necessary;*

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

4 ~~*(14)(12) perform such other functions and duties as provided by law*~~
 5 ~~*and as directed by the CISO.*~~

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

14 *(2) Results of audits conducted pursuant to subsection ~~(e)(8)~~ (c)(5)*
 15 *and the reports described in subsection (d)(1) shall be confidential and*
 16 *shall not be subject to discovery or disclosure pursuant to the open records*
 17 *act, K.S.A. 45-215 et seq., and amendments thereto. ~~The provisions of this~~*
 18 ~~*subsection shall expire on July 1, 2028, unless the legislature reviews and*~~
 19 ~~*acts to continue such provision pursuant to K.S.A. 45-229, and*~~
 20 ~~*amendments thereto, prior to July 1, 2028.*~~

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

26 Sec. 25. K.S.A. 2023 Supp. 75-7240 is hereby amended to read as
 27 follows: 75-7240. (a) The executive branch agency heads shall:

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

- 31 ~~(A) Agency sites;~~
- 32 ~~(B) agency real property;~~
- 33 ~~(C) infrastructure in state data centers;~~
- 34 ~~(D) third-party locations; and~~
- 35 ~~(E) in transit between locations;~~

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

38 ~~(3)(2) designate an information security officer to administer the~~
 39 ~~agency's information security program that reports directly to executive~~
 40 ~~leadership;~~

41 ~~(4)(3) participate in CISO-sponsored statewide cybersecurity program~~
 42 ~~initiatives and services;~~

43 ~~(5) implement policies and standards to ensure that all the agency's~~

1 data and information technology resources are maintained in compliance
2 with applicable state and federal laws and rules and regulations;

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

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

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

15 ~~(B) ensure that the agency conducts annual internal assessments of its~~
16 ~~security program. Internal assessment results shall be considered~~
17 ~~confidential and shall not be subject to discovery by or release to any~~
18 ~~person or agency, outside of the KISO or CISO, without authorization~~
19 ~~from the executive branch agency director or head; and~~

20 ~~(C) prepare or have prepared a financial summary identifying~~
21 ~~cybersecurity expenditures addressing the findings of the cybersecurity~~
22 ~~self-assessment report required in subparagraph (A), excluding~~
23 ~~information that might put the data or information resources of the agency~~
24 ~~or its contractors at risk and submit such report to the house of~~
25 ~~representatives committee on appropriations and the senate committee on~~
26 ~~ways and means; and~~

27 ~~(9)(4) ensure that if an agency owns, licenses or maintains~~
28 ~~computerized data that includes personal information, confidential~~
29 ~~information or information, the disclosure of which is regulated by law,~~
30 ~~such agency shall, in the event of a breach or suspected breach of system~~
31 ~~security or an unauthorized exposure of that information:~~

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

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

38 ~~(i) The CISO; and~~

39 ~~(ii) if the breach, suspected breach or unauthorized exposure involves~~
40 ~~election data, the secretary of state.~~

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

42 ~~(1) Participate in annual agency leadership training to ensure~~
43 ~~understanding of:~~

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

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

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

7 (D) steps to be undertaken by the executive director or agency head
8 and agency employees to protect their information and information
9 systems; *and*

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

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

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

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

31 Sec. 26. K.S.A. 40-110, 75-413, 75-623, 75-710, 75-711 and 75-7203
32 and K.S.A. 2023 Supp. 45-229, 75-7201, 75-7202, 75-7205, 75-7206, 75-
33 7208, 75-7209, 75-7237, 75-7238, 75-7239 and 75-7240 are hereby
34 repealed.

35 Sec. 27. This act shall take effect and be in force from and after its
36 publication in the statute book.