

HOUSE BILL No. 2548

By Joint Committee on Information Technology

1-25

1 AN ACT concerning information technology; relating to information
2 technology projects and reporting requirements; information
3 technology security training and cybersecurity reports; requiring certain
4 information to be provided to the joint committee on information
5 technology; amending K.S.A. 46-2102, 75-7201, 75-7205, 75-7206,
6 75-7208, 75-7209, 75-7210, 75-7211, 75-7237, 75-7239, 75-7240 and
7 75-7242 and repealing the existing sections.

8
9 *Be it enacted by the Legislature of the State of Kansas:*

10 Section 1. K.S.A. 46-2102 is hereby amended to read as follows: 46-
11 2102. In addition to other powers and duties authorized or prescribed by
12 law or by the legislative coordinating council, the joint committee on
13 information technology shall:

14 (a) Study the use by state agencies and institutions of computers,
15 telecommunications and other information technologies;

16 (b) review new governmental computer hardware and software
17 acquisition, information storage, transmission, processing and
18 telecommunications technologies proposed by state agencies and
19 institutions, and the implementation plans therefor, including all
20 information technology project budget estimates and three-year strategic
21 information technology plans that are submitted to the joint committee
22 pursuant to K.S.A. 2000-Supp. 75-7210, and amendments thereto;

23 (c) *advise and consult on all state agency information technology*
24 *projects, as defined in K.S.A. 75-7201, and amendments thereto, that pose*
25 *a significant business risk as determined by the information technology*
26 *executive council's policies and in accordance with K.S.A. 75-7209, and*
27 *amendments thereto;*

28 (d) make recommendations on all such implementation plans, budget
29 estimates, *requests for proposals for information technology projects* and
30 three-year plans to the ways and means committee of the senate and the
31 committee on appropriations of the house of representatives;

32 ~~(d)~~(e) study the progress and results of all newly implemented
33 governmental computer hardware and software, information storage,
34 transmission, processing and telecommunications technologies of state
35 agencies and institutions including all information technology projects for
36 state agencies which have been authorized or for which appropriations

1 have been approved by the legislature; and

2 (e)(f) make an annual report to the legislative coordinating council as
3 provided in K.S.A. 46-1207, and amendments thereto, and such special
4 reports to committees of the house of representatives and senate as are
5 deemed appropriate by the joint committee.

6 Sec. 2. K.S.A. 75-7201 is hereby amended to read as follows: 75-
7 7201. As used in K.S.A. 75-7201 through 75-7212, and amendments
8 thereto:

9 (a) *"Business risk" means the overall level of risk determined by a*
10 *business risk assessment that includes, but is not limited to, cost,*
11 *information security and other elements as determined by the information*
12 *technology executive council's policies.*

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

17 (b)(c) *"Executive agency" means any state agency in the executive*
18 *branch of government.*

19 (e)(d) ~~"Information technology project" means a project for a major~~
20 ~~computer, telecommunications or other information technology~~
21 ~~improvement with an estimated cumulative cost of \$250,000 or more and~~
22 ~~includes any such project that has proposed expenditures for: (1) New or~~
23 ~~replacement equipment or software; (2) upgrade improvements to existing~~
24 ~~equipment and any computer systems, programs or software upgrades~~
25 ~~therefor; or (3) data or consulting or other professional services for such a~~
26 ~~project an information technology effort by a state agency of defined and~~
27 ~~limited duration that implements, effects a change in or presents a risk to~~
28 ~~processes, services, security, systems, records, data, human resources or~~
29 ~~architecture.~~

30 (d)(e) *"Information technology project change or overrun" means any*
31 *of the following any change in:*

32 (1) ~~Any change in~~ Planned expenditures for an information
33 technology project that would result in the total authorized cost of the
34 project being increased above the currently authorized cost of such project
35 by more than ~~either \$1,000,000 or 10% of such currently authorized cost~~
36 ~~of such project, whichever is lower or an established threshold within the~~
37 ~~information technology executive council's policies;~~

38 (2) ~~any change in~~ the scope or project timeline of an information
39 technology project, as such scope was presented to and reviewed by the
40 joint committee or the chief information technology officer to whom the
41 project was submitted pursuant to K.S.A. 75-7209, and amendments
42 thereto, *that is a change of more than 10% or a change that is significant*
43 *as determined by the information technology executive council's policies;*

1 or

2 (3) ~~any change in~~ the proposed use of any new or replacement
3 information technology equipment or in the use of any existing
4 information technology equipment that has been significantly upgraded.

5 ~~(e)~~(f) "Joint committee" means the joint committee on information
6 technology.

7 ~~(f)~~(g) "Judicial agency" means any state agency in the judicial branch
8 of government.

9 ~~(g)~~(h) "Legislative agency" means any state agency in the legislative
10 branch of government.

11 ~~(h)~~(i) "Project" means a planned series of events or activities that is
12 intended to accomplish a specified outcome in a specified time period,
13 under consistent management direction within a state agency or shared
14 among two or more state agencies, and that has an identifiable budget for
15 anticipated expenses.

16 ~~(i)~~(j) "Project completion" means the date and time when the head of
17 a state agency having primary responsibility for an information technology
18 project certifies that the improvement being produced or altered under the
19 project is ready for operational use.

20 ~~(j)~~(k) "Project start" means the date and time when a state agency
21 begins a formal study of a business process or technology concept to
22 assess the needs of the state agency, determines project feasibility or
23 prepares an information technology project budget estimate under K.S.A.
24 75-7209, and amendments thereto.

25 ~~(k)~~(l) "State agency" means any state office or officer, department,
26 board, commission, institution or bureau, or any agency, division or unit
27 thereof.

28 Sec. 3. K.S.A. 75-7205 is hereby amended to read as follows: 75-
29 7205. (a) There is hereby established within and as a part of the office of
30 information technology services the position of executive chief
31 information technology officer. The executive chief information
32 technology officer shall be in the unclassified service under the Kansas
33 civil service act, shall be appointed by the governor, and shall receive
34 compensation in an amount fixed by the governor. The executive chief
35 information technology officer shall maintain a presence in any cabinet
36 established by the governor and shall report to the governor.

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

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

1 resource policies and procedures and project management methodologies
2 adopted by the information technology executive council; (B) the
3 information technology architecture adopted by the information
4 technology executive council; (C) the standards for data management
5 adopted by the information technology executive council; and (D) the
6 strategic information technology management plan adopted by the
7 information technology executive council;

8 (2) report to the chief information technology architect all deviations
9 from the state information architecture that are reported to the executive
10 information technology officer by executive agencies;

11 (3) submit recommendations to the division of the budget as to the
12 technical and management merit of information technology ~~project~~
13 ~~estimates~~ *projects* and information technology project changes and
14 overruns submitted by executive agencies *that are reportable* pursuant to
15 K.S.A. 75-7209, and amendments thereto, ~~based on the determinations~~
16 ~~made pursuant to subsection (b)(1);~~

17 (4) monitor executive agencies' compliance with: (A) The
18 information technology resource policies and procedures and project
19 management methodologies adopted by the information technology
20 executive council; (B) the information technology architecture adopted by
21 the information technology executive council; (C) the standards for data
22 management adopted by the information technology executive council;
23 and (D) the strategic information technology management plan adopted by
24 the information technology executive council;

25 (5) coordinate implementation of new information technology among
26 executive agencies and with the judicial and legislative chief information
27 technology officers;

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

31 (7) perform such other functions and duties as provided by law or as
32 directed by the governor.

33 Sec. 4. K.S.A. 75-7206 is hereby amended to read as follows: 75-
34 7206. (a) There is hereby established within and as a part of the office of
35 the state judicial administrator the position of judicial chief information
36 technology officer. The judicial chief information technology officer shall
37 be appointed by the judicial administrator, subject to approval of the chief
38 justice, and shall receive compensation determined by the judicial
39 administrator, subject to approval of the chief justice.

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

41 (1) Review and consult with each judicial agency regarding
42 information technology plans, deviations from the state information
43 technology architecture, information technology project estimates and

1 information technology project changes and overruns submitted by such
2 agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine
3 whether the agency has complied with: (A) The information technology
4 resource policies and procedures and project management methodologies
5 adopted by the information technology executive council; (B) the
6 information technology architecture adopted by the information
7 technology executive council; (C) the standards for data management
8 adopted by the information technology executive council; and (D) the
9 strategic information technology management plan adopted by the
10 information technology executive council;

11 (2) report to the chief information technology architect all deviations
12 from the state information architecture that are reported to the judicial
13 information technology officer by judicial agencies;

14 (3) submit recommendations to the judicial administrator as to the
15 technical and management merit of information technology ~~project~~
16 ~~estimates~~ *projects* and information technology project changes and
17 overruns submitted by judicial agencies *that are reportable* pursuant to
18 K.S.A. 75-7209, and amendments thereto, ~~based on the determinations~~
19 ~~pursuant to subsection (b)(1)~~;

20 (4) monitor judicial agencies' compliance with: (A) The information
21 technology resource policies and procedures and project management
22 methodologies adopted by the information technology executive council;
23 (B) the information technology architecture adopted by the information
24 technology executive council; (C) the standards for data management
25 adopted by the information technology executive council; and (D) the
26 strategic information technology management plan adopted by the
27 information technology executive council;

28 (5) coordinate implementation of new information technology among
29 judicial agencies and with the executive and legislative chief information
30 technology officers;

31 (6) designate the ownership of information resource processes and the
32 lead agency for implementation of new technologies and networks shared
33 by multiple agencies within the judicial branch of state government; and

34 (7) perform such other functions and duties as provided by law or as
35 directed by the judicial administrator.

36 Sec. 5. K.S.A. 75-7208 is hereby amended to read as follows: 75-
37 7208. The legislative chief information technology officer shall:

38 (a) Review and consult with each legislative agency regarding
39 information technology plans, deviations from the state information
40 technology architecture, information technology project estimates and
41 information technology project changes and overruns submitted by such
42 agency pursuant to K.S.A. 75-7209, and amendments thereto, to determine
43 whether the agency has complied with:

1 (1) The information technology resource policies and procedures and
 2 project management methodologies adopted by the information technology
 3 executive council;

4 (2) the information technology architecture adopted by the
 5 information technology executive council;

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

8 (4) the strategic information technology management plan adopted by
 9 the information technology executive council;

10 (b) report to the chief information technology architect all deviations
 11 from the state information architecture that are reported to the legislative
 12 information technology officer by legislative agencies;

13 (c) submit recommendations to the legislative coordinating council as
 14 to the technical and management merit of information technology ~~project~~
 15 ~~estimates~~ *projects* and information technology project changes and
 16 overruns submitted by legislative agencies *that are reportable* pursuant to
 17 K.S.A. 75-7209, and amendments thereto, ~~based on the determinations~~
 18 ~~pursuant to subsection (a)~~;

19 (d) monitor legislative agencies' compliance with *the*:

20 (1) ~~The~~ Information technology resource policies and procedures and
 21 project management methodologies adopted by the information technology
 22 executive council;

23 (2) ~~the~~ information technology architecture adopted by the
 24 information technology executive council;

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

27 (4) ~~the~~ strategic information technology management plan adopted by
 28 the information technology executive council;

29 (e) coordinate implementation of new information technology among
 30 legislative agencies and with the executive and judicial chief information
 31 technology officers;

32 (f) designate the ownership of information resource processes and the
 33 lead agency for implementation of new technologies and networks shared
 34 by multiple agencies within the legislative branch of state government;

35 (g) serve as staff of the joint committee; and

36 (h) perform such other functions and duties as provided by law or as
 37 directed by the legislative coordinating council or the joint committee.

38 Sec. 6. K.S.A. 75-7209 is hereby amended to read as follows: 75-
 39 7209. (a) (1) Whenever an agency proposes an information technology
 40 project, such agency shall prepare and submit *information technology*
 41 *project documentation* to the chief information technology officer of the
 42 branch of state government of which the agency is a part ~~of a project~~
 43 ~~budget estimate therefor, and for each amendment or revision thereof, in~~

1 accordance with this section. Each information technology project budget
2 estimate shall be in such form as required by the director of the budget, in
3 consultation with the chief information technology architect, and by this
4 section. In each case, the agency shall prepare and include as a part of such
5 project budget estimate a plan consisting of a written program statement
6 describing the project. The program statement shall:

7 (1) Include a detailed description of and justification for the project,
8 including: (A) An analysis of the programs, activities and other needs and
9 intended uses for the additional or improved information technology; (B) a
10 statement of project scope including identification of the organizations and
11 individuals to be affected by the project and a definition of the
12 functionality to result from the project; and (C) an analysis of the
13 alternative means by which such information technology needs and uses
14 could be satisfied;

15 (2) describe the tasks and schedule for the project and for each phase
16 of the project, if the project is to be completed in more than one phase;

17 (3) include a financial plan showing: (A) The proposed source of
18 funding and categorized expenditures for each phase of the project; and
19 (B) cost estimates for any needs analyses or other investigations,
20 consulting or other professional services, computer programs, data,
21 equipment, buildings or major repairs or improvements to buildings and
22 other items or services necessary for the project; and

23 (4) include a cost-benefit statement based on an analysis of
24 qualitative as well as financial benefits. *Such information technology
25 project documentation shall:*

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

32 (B) *be consistent with the information technology executive council's
33 policies.*

34 (2) *Any information technology project with significant business risk,
35 as determined pursuant to the information technology executive council's
36 policies, shall be presented to the joint committee on information
37 technology by such branch chief information technology officer.*

38 (b) (1) ~~Before one or more state agencies proposing an information
39 technology project begin implementation of the project, the project plan,
40 including the architecture and the cost-benefit analysis, shall be approved
41 by the head of each state agency proposing the project and by the chief
42 information technology officer of each branch of state government of
43 which the agency or agencies are a part. Approval of those projects that~~

1 involve telecommunications services shall also be subject to the provisions
2 of K.S.A. 75-4709, 75-4710 and 75-4712, and amendments thereto.

3 ~~(2) All specifications for bids or proposals related to an approved~~
4 ~~information technology project of one or more state agencies shall be~~
5 ~~reviewed by the chief information technology officer of each branch of~~
6 ~~state government of which the agency or agencies are a part Prior to the~~
7 ~~release of any request for proposal for an information technology project~~
8 ~~with significant business risk:~~

9 (A) Specifications for bids or proposals for such project shall be
10 submitted to the chief information technology officer of the branch of state
11 government of which the agency or agencies are a part. Information
12 technology projects requiring chief information technology officer
13 approval shall also require the chief information technology officer's
14 written approval on specifications for bids or proposals; and

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

1 at a meeting.

2 (ii) The state agency or agencies shall be deemed to have advised
3 and consulted with the joint committee about such proposed release of any
4 request for proposal or other bid event for an information technology
5 project and may authorize or approve such proposed release of any
6 request for proposal or other bid event for an information technology
7 project if:

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

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

18 ~~(2)~~(A) Agencies are prohibited from contracting with a vendor to
19 implement the project if that vendor prepared or assisted in the preparation
20 of the program statement ~~required under subsection (a)~~, the project
21 planning documents ~~required under subsection (b)(1)~~; or any other project
22 plans prepared prior to the project being approved by the chief information
23 technology officer as required ~~under subsection (b)(1)~~ by this section.

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

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

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

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

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

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

41 Sec. 7. K.S.A. 75-7210 is hereby amended to read as follows: 75-
42 7210. (a) Not later than ~~October~~ November 1 of each year, the executive,
43 judicial and legislative chief information technology officers shall submit

1 to the joint committee and to the legislative research department all
2 information technology project budget estimates and amendments and
3 revisions thereto, all three-year plans and all deviations from the state
4 information technology architecture submitted to such officers pursuant to
5 K.S.A. 75-7209, and amendments thereto. The legislative chief
6 information technology officer *of the branch of state government of which*
7 *each such agency is a part* shall review all such estimates and amendments
8 and revisions thereto, plans and deviations and shall make
9 recommendations to the joint committee regarding the merit thereof and
10 appropriations therefor.

11 (b) The executive and judicial chief information technology officers
12 shall report to the legislative chief information technology officer, at times
13 agreed upon by the three officers:

14 (1) Progress regarding implementation of information technology
15 projects of state agencies within the executive and judicial branches of
16 state government; and

17 (2) all proposed expenditures for such projects, including all revisions
18 to such proposed expenditures, for the current fiscal year and for ensuing
19 fiscal years.

20 Sec. 8. K.S.A. 75-7211 is hereby amended to read as follows: 75-
21 7211. (a) The legislative chief information technology officer, under the
22 direction of the joint committee, shall monitor state agency execution of
23 *reported* information technology projects and, at times agreed upon by the
24 three chief information technology officers, shall report progress regarding
25 the implementation of such projects and all proposed expenditures
26 therefor, including all revisions to such proposed expenditures for the
27 current fiscal year and for ensuing fiscal years.

28 (b) *For information technology projects, the joint committee may:*

29 (1) ~~Require the head of a any state agency with primary responsibility~~
30 ~~for an information technology project may authorize or approve, without~~
31 ~~prior consultation with the joint committee, any change in planned~~
32 ~~expenditures for an information technology project that would result in the~~
33 ~~total cost of the project being increased above the currently authorized cost~~
34 ~~of such project but that increases the total cost of such project by less than~~
35 ~~the lower of either \$1,000,000 or 10% of the currently authorized cost, and~~
36 ~~any change in planned expenditures for an information technology project~~
37 ~~involving a cost reduction, other than a change in the proposed use of any~~
38 ~~new or replacement information technology equipment or in the use of any~~
39 ~~existing information technology equipment that has been significantly~~
40 ~~upgraded to advise and consult on the status and progress of such~~
41 ~~information technology project, including revisions to expenditures for the~~
42 ~~current fiscal year and ensuing fiscal years; and~~

43 (2) *report on the status and progress of such information technology*

1 *projects to the senate standing committee on ways and means, the house of*
 2 *representatives standing committee on appropriations and the legislative*
 3 *budget committee.*

4 (c) *Prior to authorizing or approving any information technology*
 5 *project change or overrun, the head of a state agency with primary*
 6 *responsibility for—~~an~~ such information technology project shall ~~not~~*
 7 *~~authorize or approve, without first advising and consulting with the joint~~*
 8 *~~committee any information technology project change or overrun report~~*
 9 *all such information technology project changes or overruns to the joint*
 10 *committee through the chief information technology officer of the branch*
 11 *of state government of which the agency is a part pursuant to the*
 12 *information technology executive council's policy. The joint committee*
 13 *shall report all such changes and overruns to the senate standing*
 14 *committee on ways and means—and, the house of representatives standing*
 15 *committee on appropriations and the legislative budget committee.*

16 Sec. 9. K.S.A. 75-7237 is hereby amended to read as follows: 75-
 17 7237. As used in K.S.A. 75-7236 through 75-7243, and amendments
 18 thereto:

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

20 (b) "Breach" or "breach of security" means unauthorized access of
 21 data in electronic form containing personal information. Good faith access
 22 of personal information by an employee or agent of an executive branch
 23 agency does not constitute a breach of security, provided that the
 24 information is not used for a purpose unrelated to the business or subject to
 25 further unauthorized use.

26 (c) "CISO" means the executive branch chief information security
 27 officer.

28 (d) "Cybersecurity" is the body of information technologies,
 29 processes and practices designed to protect networks, computers, programs
 30 and data from attack, damage or unauthorized access.

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

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

36 (g) "Executive branch agency" means any agency in the executive
 37 branch of the state of Kansas, but does not include elected office agencies,
 38 the adjutant general's department, the Kansas public employees retirement
 39 system, regents' institutions, or the board of regents.

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

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

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

1 individual:

2 (i) Social security number;

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

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

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

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

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

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

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

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

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

26 Sec. 10. K.S.A. 75-7239 is hereby amended to read as follows: 75-
27 7239. (a) There is hereby established within and as a part of the office of
28 information technology services the Kansas information security office.
29 The Kansas information security office shall be administered by the CISO
30 and be staffed appropriately to effect the provisions of the Kansas
31 cybersecurity act.

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

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

- 1 (1) Administer the Kansas cybersecurity act;
- 2 (2) assist the executive branch in developing, implementing and
3 monitoring strategic and comprehensive information security risk-
4 management programs;
- 5 (3) facilitate executive branch information security governance,
6 including the consistent application of information security programs,
7 plans and procedures;
- 8 (4) using standards adopted by the information technology executive
9 council, create and manage a unified and flexible control framework to
10 integrate and normalize requirements resulting from applicable state and
11 federal laws, and rules and regulations;
- 12 (5) facilitate a metrics, logging and reporting framework to measure
13 the efficiency and effectiveness of state information security programs;
- 14 (6) provide the executive branch strategic risk guidance for
15 information technology projects, including the evaluation and
16 recommendation of technical controls;
- 17 (7) assist in the development of executive branch agency
18 cybersecurity programs ~~that are in~~ *to ensure* compliance with applicable
19 state and federal laws and rules and regulations and standards adopted by
20 the information technology executive council;
- 21 (8) coordinate the use of external resources involved in information
22 security programs, including, but not limited to, interviewing and
23 negotiating contracts and fees;
- 24 (9) liaise with external agencies, such as law enforcement and other
25 advisory bodies as necessary, to ensure a strong security posture;
- 26 (10) assist in the development of plans and procedures to manage and
27 recover business-critical services in the event of a cyberattack or other
28 disaster;
- 29 (11) assist executive branch agencies to create a framework for roles
30 and responsibilities relating to information ownership, classification,
31 accountability and protection;
- 32 (12) ensure a cybersecurity ~~training program is provided to executive~~
33 ~~branch agencies at no cost to the agencies~~ *awareness training program is*
34 *made available to all branches of state government; and*
- 35 (13) ~~provide cybersecurity threat briefings to the information~~
36 ~~technology executive council;~~
- 37 (14) ~~provide an annual status report of executive branch cybersecurity~~
38 ~~programs of executive branch agencies to the joint committee on~~
39 ~~information technology and the house committee on government,~~
40 ~~technology and security; and~~
- 41 ~~(15)~~ perform such other functions and duties as provided by law and
42 as directed by the CISO.

43 Sec. 11. K.S.A. 75-7240 is hereby amended to read as follows: 75-

1 7240. (a) The executive branch agency heads shall:

2 (a)(1) Be solely responsible for security of all data and information
3 technology resources under such agency's purview, irrespective of the
4 location of the data or resources. Locations of data may include:

5 (1)(A) Agency sites;

6 (2)(B) agency real property;

7 (3)(C) infrastructure in state data centers;

8 (4)(D) third-party locations; and

9 (5)(E) in transit between locations;

10 (b)(2) ensure that an agency-wide information security program is in
11 place;

12 (c)(3) designate an information security officer to administer the
13 agency's information security program that reports directly to executive
14 leadership;

15 (d)(4) participate in CISO-sponsored statewide cybersecurity program
16 initiatives and services;

17 (e)(5) implement policies and standards to ensure that all the agency's
18 data and information technology resources are maintained in compliance
19 with applicable state and federal laws and rules and regulations;

20 (f)(6) implement appropriate cost-effective safeguards to reduce,
21 eliminate or recover from identified threats to data and information
22 technology resources;

23 (g)(7) include all appropriate cybersecurity requirements in the
24 agency's request for proposal specifications for procuring data and
25 information technology systems and services;

26 (h) ~~(1)(8) (A) submit a cybersecurity assessment self-assessment~~
27 report to the CISO by October 16 of each even-numbered year, including
28 an executive summary of the findings, that assesses the extent to which a
29 ~~computer, a computer program, a computer network, a computer system, a~~
30 ~~printer, an interface to a computer system, including mobile and peripheral~~
31 ~~devices, computer software, or the data processing of the agency or of a~~
32 ~~contractor~~ of the agency is vulnerable to unauthorized access or harm,
33 including the extent to which the agency's or contractor's electronically
34 stored information is vulnerable to alteration, damage, erasure or
35 inappropriate use;

36 (2)(B) ensure that the agency conducts annual internal assessments of
37 its security program. Internal assessment results shall be considered
38 confidential and shall not be subject to discovery by or release to any
39 person or agency, outside of the KISO or CISO, *without authorization*
40 *from the executive branch agency director or head*. This provision
41 regarding confidentiality shall expire on July 1, 2023, unless the
42 legislature reviews and reenacts such provision pursuant to K.S.A. 45-229,
43 and amendments thereto, prior to July 1, 2023; and

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

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

20 ~~(j)(9)~~ ensure that if an agency owns, licenses or maintains
 21 computerized data that includes personal information, confidential
 22 information or information, the disclosure of which is regulated by law,
 23 such agency shall, in the event of a breach or suspected breach of system
 24 security or an unauthorized exposure of that information:

25 ~~(4)(A)~~ Comply with the notification requirements set out in K.S.A.
 26 2021 Supp. 50-7a01 et seq., and amendments thereto, and applicable
 27 federal laws and rules and regulations, to the same extent as a person who
 28 conducts business in this state; and

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

33 (b) *The director or head of all state agencies shall:*

34 (1) *Participate in annual agency leadership training to ensure*
 35 *understanding of:*

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

38 (B) *how cyberattacks and data breaches on the agency's operations*
 39 *and assets may impact the operations and assets of other governmental*
 40 *entities on the state enterprise network;*

41 (C) *how cyberattacks and data breaches occur; and*

42 (D) *steps to be undertaken by the executive director or agency head*
 43 *and agency employees to protect their information and information*

1 systems;

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

5 (3) require that all employees with access to information technology
6 receive a minimum of one hour of information technology security training
7 per year.

8 (c) (1) The CISO, with input from the joint committee on information
9 technology and the joint committee on Kansas security, shall develop a
10 self-assessment report template for use under subsection (a)(8)(A). The
11 most recent version of such template shall be made available to state
12 agencies prior to July 1 of each even-numbered year. The CISO shall
13 aggregate data from the self-assessments received under subsection (a)(8)
14 (A) and provide a summary of such data to the joint committee on
15 information technology and the joint committee on Kansas security.

16 (2) Self-assessment reports made to the CISO pursuant to subsection
17 (a)(8)(A) shall be confidential and shall not be subject to the provisions of
18 the Kansas open records act, K.S.A. 45-215 et seq., and amendments
19 thereto. The provisions of this paragraph shall expire on July 1, 2027,
20 unless the legislature reviews and reenacts this provision pursuant to
21 K.S.A. 45-229, and amendments thereto, prior to July 1, 2027.

22 Sec. 12. K.S.A. 75-7242 is hereby amended to read as follows: 75-
23 7242. Information collected to effectuate this act shall be considered
24 confidential by ~~the executive branch agency and KISO~~ all state and local
25 government organizations unless all data elements or information that
26 specifically identifies a target, vulnerability or weakness that would place
27 the organization at risk have been redacted, including: (a) System
28 information logs; (b) vulnerability reports; (c) risk assessment reports; (d)
29 system security plans; (e) detailed system design plans; (f) network or
30 system diagrams; and (g) audit reports. The provisions of this section shall
31 expire on July 1, 2023, unless the legislature reviews and reenacts this
32 provision pursuant to K.S.A. 45-229, and amendments thereto, prior to
33 July 1, 2023.

34 Sec. 13. K.S.A. 46-2102, 75-7201, 75-7205, 75-7206, 75-7208, 75-
35 7209, 75-7210, 75-7211, 75-7237, 75-7239, 75-7240 and 75-7242 are
36 hereby repealed.

37 Sec. 14. This act shall take effect and be in force from and after its
38 publication in the statute book.