

Substitute for HOUSE BILL No. 2077

By Committee on Appropriations

2-9

1 AN ACT concerning information technology; requiring reporting of
2 significant cybersecurity incidents; changing membership, terms and
3 quorum requirements for the information technology executive council;
4 relating to information technology projects and reporting requirements;
5 information technology security training and cybersecurity reports;
6 duties of the chief information security officer; requiring certain
7 information to be provided to the joint committee on information
8 technology; amending K.S.A. 46-2102, {74-5704,} 75-7201, 75-7202,
9 75-7205, 75-7206, 75-7208, 75-7209, 75-7210, 75-7211, 75-7237, 75-
10 7238, 75-7239, 75-7240 and 75-7242 and repealing the existing
11 sections.
12

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

14 New Section 1. (a) **{Except as provided in subsection (b),}** any
15 entity that transmits, receives, processes or stores personal information that
16 is provided by the state of Kansas or supports information systems
17 operated by the state of Kansas or any governmental entity that accesses
18 information systems operated by the state of Kansas that has a significant
19 cybersecurity incident shall, not later than 12 hours after the discovery of
20 the significant cybersecurity incident, notify the Kansas information
21 security office and, if the significant cybersecurity incident involves
22 election data, the secretary of state.

23 (b) (1) **{ Any entity that is connected to the Kansas criminal justice**
24 **information system shall report any cybersecurity incident in**
25 **accordance with rules and regulations adopted by the Kansas criminal**
26 **justice information system committee pursuant to K.S.A. 74-5704, and**
27 **amendments thereto.}**

28 **{(2) An entity that is connected to the Kansas criminal justice**
29 **information system and is not connected to any other state of Kansas**
30 **information system shall not be required to make the report required**
31 **in subsection (a).}**

32 **{(3) The Kansas bureau of investigation shall notify the Kansas**
33 **information security office of any significant cybersecurity incident**
34 **report it receives in accordance with rules and regulations adopted**
35 **pursuant to K.S.A. 74-5704, and amendments thereto, not later than**
36 **12 hours after receipt of such report.}**

1 ~~{(c)(1)}~~ **{(c)(1)}** The information provided pursuant to ~~subsection (a)~~ **{this**
2 **section}** shall only be shared with individuals who need to know such
3 information for response and defensive activities to preserve the integrity
4 of state information systems and networks or to provide assistance if
5 requested.

6 (2) Such information shall be confidential and shall not be subject to
7 disclosure pursuant to the open records act, K.S.A. 45-215 et seq., and
8 amendments thereto. This paragraph shall expire on July 1, 2028, unless
9 the legislature reviews and acts to continue such provision pursuant to
10 K.S.A. 45-229, and amendments thereto, prior to July 1, 2028.

11 (3) The Kansas information security office shall only report the
12 information provided pursuant to ~~subsection (a)~~ **{this section}** as
13 aggregate data.

14 ~~{(d)}~~ **{(d)}** For the purposes of this section, "significant cybersecurity
15 incident" means a cybersecurity event, incident, breach, suspected breach
16 or unauthorized ~~disclosure~~ **{disclosure}** that requires the entity to initiate
17 a response or recovery.

18 Sec. 2. K.S.A. 46-2102 is hereby amended to read as follows: 46-
19 2102. In addition to other powers and duties authorized or prescribed by
20 law or by the legislative coordinating council, the joint committee on
21 information technology shall:

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

24 (b) review new governmental computer hardware and software
25 acquisition, information storage, transmission, processing and
26 telecommunications technologies proposed by state agencies and
27 institutions, and the implementation plans therefor, including all
28 information technology project budget estimates and three-year strategic
29 information technology plans that are submitted to the joint committee
30 pursuant to K.S.A. 75-7210, and amendments thereto;

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

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

40 ~~{(e)}~~ **{(e)}** study the progress and results of all newly implemented
41 governmental computer hardware and software, information storage,
42 transmission, processing and telecommunications technologies of state
43 agencies and institutions including all information technology projects for

1 state agencies which have been authorized or for which appropriations
2 have been approved by the legislature; and

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

7 **{Sec. 3. K.S.A. 74-5704 is hereby amended to read as follows: 74-
8 5704. The committee shall:**

9 (a) ~~Adopt and enforce such rules, regulations and policies as that~~
10 **are necessary for the establishment, maintenance, upgrading and**
11 **operation of the statewide criminal justice information system; and**

12 (b) *adopt rules and regulations that require entities connected to the*
13 *Kansas criminal justice information system to report any cybersecurity*
14 *incident to the Kansas bureau of investigation not later than 12 hours*
15 *after the discovery of such cybersecurity incident.}*

16 ~~Sec. 3. {4.}~~ K.S.A. 75-7201 is hereby amended to read as follows: 75-
17 7201. As used in K.S.A. 75-7201 through 75-7212, and amendments
18 thereto:

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

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

27 ~~(b)(c)~~ *"Executive agency" means any state agency in the executive*
28 *branch of government.*

29 ~~(e)(d)~~ *"Information technology project" means a project for a major*
30 ~~computer, telecommunications or other information technology~~
31 ~~improvement with an estimated cumulative cost of \$250,000 or more and~~
32 ~~includes any such project that has proposed expenditures for: (1) New or~~
33 ~~replacement equipment or software; (2) upgrade improvements to existing~~
34 ~~equipment and any computer systems, programs or software upgrades~~
35 ~~therefor; or (3) data or consulting or other professional services for such a~~
36 ~~project an information technology effort by a state agency of defined and~~
37 ~~limited duration that implements, effects a change in or presents a risk to~~
38 ~~processes, services, security, systems, records, data, human resources or~~
39 ~~architecture.~~

40 ~~(d)(e)~~ *"Information technology project change or overrun" means any*
41 *of the following any change in:*

42 (1) ~~Any change in~~ Planned expenditures for an information
43 technology project that would result in the total authorized cost of the

1 project being increased above the currently authorized cost of such project
2 by more than ~~either \$1,000,000 or 10%~~ of such currently authorized cost
3 of such project, ~~whichever is lower~~ *or an established threshold within the*
4 *information technology executive council's policies;*

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

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

15 ~~(e)~~(f) "Joint committee" means the joint committee on information
16 technology.

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

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

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

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

30 ~~(j)~~(k) "Project start" means the date and time when a state agency
31 begins a formal study of a business process or technology concept to
32 assess the needs of the state agency, determines project feasibility or
33 prepares an information technology project budget estimate under K.S.A.
34 75-7209, and amendments thereto.

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

38 ~~Sec. 4. {5.}~~ K.S.A. 75-7202 is hereby amended to read as follows: 75-
39 7202. (a) There is hereby established the information technology executive
40 council which shall be attached to the office of information technology
41 services for purposes of administrative functions.

42 (b) (1) The council shall be composed of 17 voting members as
43 follows:

- 1 (A) Two cabinet agency heads or such persons' designees;
2 (B) two noncabinet agency heads or such persons' designees;
3 (C) the executive chief information technology officer;
4 (D) the legislative chief information technology officer;
5 (E) the judicial chief information technology officer;
6 (F) the chief executive officer of the state board of regents or such
7 person's designee;
8 (G) one representative of cities;
9 (H) one representative of counties; the network manager of the
10 information network of Kansas (INK);
11 (I) one representative with background and knowledge in technology
12 and cybersecurity from the private sector, ~~however, except that~~ such
13 representative or such representative's employer shall not be an
14 information technology or cybersecurity vendor that does business with
15 the state of Kansas;
16 (J) one representative appointed by the Kansas criminal justice
17 information system committee;
18 (K) one member of the ~~senate ways and means committee~~ appointed
19 by the president of the senate or such member's designee;
20 (L) one member of the ~~senate ways and means committee~~ appointed
21 by the minority leader of the senate or such member's designee;
22 (M) one member of the ~~house government, technology and security~~
23 ~~committee or its successor committee of representatives~~ appointed by the
24 speaker of the house of representatives or such member's designee; and
25 (N) one member of the ~~house government, technology and security~~
26 ~~committee or its successor committee of representatives~~ appointed by the
27 minority leader of the house of representatives or such member's designee.
28 (2) The chief information technology architect shall be a nonvoting
29 member of the council.
30 (3) The cabinet agency heads, the noncabinet agency heads, the
31 representative of cities, the representative of counties and the
32 representative from the private sector shall be appointed by the governor
33 for a term not to exceed 18 months. Upon expiration of an appointed
34 member's term, the member shall continue to hold office until the
35 appointment of a successor. *Legislative members shall remain members of*
36 *the legislature in order to retain membership on the council and shall*
37 *serve until replaced pursuant to this section. Vacancies of members during*
38 *a term shall be filled in the same manner as the original appointment only*
39 *for the unexpired part of the term. The appointing authority for a member*
40 *may remove the member, reappoint the member or substitute another*
41 *appointee for the member at any time. Nonappointed members shall serve*
42 *ex officio.*
43 (c) The chairperson of the council shall be drawn from the chief

1 information technology officers, with each chief information technology
2 officer serving a one-year term. The term of chairperson shall rotate
3 among the chief information technology officers on an annual basis.

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

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

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

16 ~~Sec. 5.~~ **{6.}** K.S.A. 75-7205 is hereby amended to read as follows: 75-
17 7205. (a) There is hereby established within and as a part of the office of
18 information technology services the position of executive chief
19 information technology officer. The executive chief information
20 technology officer shall be in the unclassified service under the Kansas
21 civil service act, shall be appointed by the governor, and shall receive
22 compensation in an amount fixed by the governor. The executive chief
23 information technology officer shall maintain a presence in any cabinet
24 established by the governor and shall report to the governor.

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

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

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

35 (B) the information technology architecture adopted by the
36 information technology executive council;

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

39 (D) the strategic information technology management plan adopted
40 by the information technology executive council;

41 (2) report to the chief information technology architect all deviations
42 from the state information architecture that are reported to the executive
43 information technology officer by executive agencies;

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

7 (4) monitor executive agencies' compliance with:

8 (A) The information technology resource policies and procedures and
9 project management methodologies adopted by the information technology
10 executive council;

11 (B) the information technology architecture adopted by the
12 information technology executive council;

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

15 (D) the strategic information technology management plan adopted
16 by the information technology executive council;

17 (5) coordinate implementation of new information technology among
18 executive agencies and with the judicial and legislative chief information
19 technology officers;

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

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

25 ~~Sec. 6.~~ {7.} K.S.A. 75-7206 is hereby amended to read as follows: 75-
26 7206. (a) There is hereby established within and as a part of the office of
27 the state judicial administrator the position of judicial chief information
28 technology officer. The judicial chief information technology officer shall
29 be appointed by the judicial administrator, subject to approval of the chief
30 justice, and shall receive compensation determined by the judicial
31 administrator, subject to approval of the chief justice.

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

33 (1) Review and consult with each judicial 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 judicial
7 information technology officer by judicial agencies;

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

14 (4) monitor judicial agencies' compliance with:

15 (A) The information technology resource policies and procedures and
16 project management methodologies adopted by the information technology
17 executive council;

18 (B) the information technology architecture adopted by the
19 information technology executive council;

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

22 (D) the strategic information technology management plan adopted
23 by the information technology executive council;

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

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

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

32 ~~Sec. 7. {8.}~~ K.S.A. 75-7208 is hereby amended to read as follows: 75-
33 7208. The legislative chief information technology officer shall:

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

40 (1) ~~The~~ Information technology resource policies and procedures and
41 project management methodologies adopted by the information technology
42 executive council;

43 (2) ~~the~~ information technology architecture adopted by the

1 information technology executive council;

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

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

6 (b) report to the chief information technology architect all deviations
7 from the state information architecture that are reported to the legislative
8 information technology officer by legislative agencies;

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

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

16 (1) ~~The~~ Information technology resource policies and procedures and
17 project management methodologies adopted by the information technology
18 executive council;

19 (2) ~~the~~ information technology architecture adopted by the
20 information technology executive council;

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

23 (4) ~~the~~ strategic information technology management plan adopted by
24 the information technology executive council;

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

28 (f) 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 legislative branch of state government;

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

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

34 Sec. 8. ~~{9.}~~ K.S.A. 75-7209 is hereby amended to read as follows: 75-
35 7209. (a) (1) Whenever an agency proposes an information technology
36 project, such agency shall prepare and submit *information technology*
37 *project documentation* to the chief information technology officer of the
38 branch of state government of which the agency is a part ~~of a project~~
39 ~~budget estimate therefor, and for each amendment or revision thereof, in~~
40 ~~accordance with this section. Each information technology project budget~~
41 ~~estimate shall be in such form as required by the director of the budget, in~~
42 ~~consultation with the chief information technology architect, and by this~~
43 ~~section. In each case, the agency shall prepare and include as a part of such~~

1 project budget estimate a plan consisting of a written program statement
2 describing the project. The program statement shall:

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

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

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

19 (4) ~~include a cost-benefit statement based on an analysis of~~
20 ~~qualitative as well as financial benefits. Such information technology~~
21 ~~project documentation shall:~~

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

28 (B) *be consistent with:*

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

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

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

35 (iv) *a strategic information technology management plan for the*
36 *state.*

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

41 (b) (1) ~~Before one or more state agencies proposing an information~~
42 ~~technology project begin implementation of the project, the project plan,~~
43 ~~including the architecture and the cost-benefit analysis, shall be approved~~

1 by the head of each state agency proposing the project and by the chief
2 information technology officer of each branch of state government of
3 which the agency or agencies are a part. Approval of those projects that
4 involve telecommunications services shall also be subject to the provisions
5 of K.S.A. 75-4709, 75-4710 and 75-4712, and amendments thereto.

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

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

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

1 subsection (b)(1)(B)(ii), the state agency shall not authorize or approve
2 the release of any request for proposal or other bid event for an
3 information technology project without having first advised and consulted
4 with the joint committee at a meeting.

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

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

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

21 ~~(3)(2)~~ (A) Agencies are prohibited from contracting with a vendor to
22 implement the project if that vendor prepared or assisted in the preparation
23 of the program statement ~~required under subsection (a)~~, the project
24 planning documents ~~required under subsection (b)(1)~~, or any other project
25 plans prepared prior to the project being approved by the chief information
26 technology officer as required ~~under subsection (b)(1)~~ by this section.

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

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

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

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

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

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

1 ~~Sec. 9. {10.}~~ K.S.A. 75-7210 is hereby amended to read as follows:
2 75-7210. ~~(a)~~ Not later than ~~October~~ *November* 1 of each year, the
3 executive, judicial and legislative chief information technology officers
4 shall submit to the joint committee and to the legislative research
5 department all information technology project budget estimates and
6 amendments and revisions thereto, all three-year plans and all deviations
7 from the state information technology architecture submitted to such
8 officers pursuant to K.S.A. 75-7209, and amendments thereto. The
9 ~~legislative chief information technology officer~~ *joint committee* shall
10 review all such estimates and amendments and revisions thereto, plans and
11 deviations and shall make recommendations to the ~~joint committee~~ *house*
12 *standing committee on appropriations and the senate standing committee*
13 *on ways and means* regarding the merit thereof and appropriations
14 therefor.

15 ~~(b) The executive and judicial chief information technology officers~~
16 ~~shall report to the legislative chief information technology officer, at times~~
17 ~~agreed upon by the three officers:~~

18 ~~(1) Progress regarding implementation of information technology~~
19 ~~projects of state agencies within the executive and judicial branches of~~
20 ~~state government; and~~

21 ~~(2) all proposed expenditures for such projects, including all revisions~~
22 ~~to such proposed expenditures, for the current fiscal year and for ensuing~~
23 ~~fiscal years.~~

24 ~~Sec. 10. {11.}~~ K.S.A. 75-7211 is hereby amended to read as follows:
25 75-7211. ~~(a) The legislative chief information technology officer, under the~~
26 ~~direction of the joint committee; shall monitor state agency execution of~~
27 ~~reported information technology projects and, at times agreed upon by.~~
28 *The joint committee shall require* the three chief information technology
29 officers, ~~shall~~ *to* report progress regarding the implementation of such
30 projects and all proposed expenditures therefor, including all revisions to
31 such proposed expenditures for the current fiscal year and for ensuing
32 fiscal years.

33 ~~(b) For information technology projects, the joint committee may:~~

34 ~~(1) Require the head of a any state agency with primary responsibility~~
35 ~~for an information technology project may authorize or approve, without~~
36 ~~prior consultation with the joint committee, any change in planned~~
37 ~~expenditures for an information technology project that would result in the~~
38 ~~total cost of the project being increased above the currently authorized cost~~
39 ~~of such project but that increases the total cost of such project by less than~~
40 ~~the lower of either \$1,000,000 or 10% of the currently authorized cost, and~~
41 ~~any change in planned expenditures for an information technology project~~
42 ~~involving a cost reduction, other than a change in the proposed use of any~~
43 ~~new or replacement information technology equipment or in the use of any~~

1 ~~existing information technology equipment that has been significantly~~
2 ~~upgraded to advise and consult on the status and progress of such~~
3 ~~information technology project, including revisions to expenditures for the~~
4 ~~current fiscal year and ensuing fiscal years; and~~

5 (2) *report on the status and progress of such information technology*
6 *projects to the senate standing committee on ways and means, the house of*
7 *representatives standing committee on appropriations and the legislative*
8 *budget committee.*

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

21 Sec. ~~H~~. {12.} K.S.A. 75-7237 is hereby amended to read as follows:
22 75-7237. As used in K.S.A. 75-7236 through 75-7243, and amendments
23 thereto:

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

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

31 (c) "CISO" means the executive branch chief information security
32 officer.

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

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

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

41 (g) "Executive branch agency" means any agency in the executive
42 branch of the state of Kansas, but does not include elected office agencies,
43 the adjutant general's department, the Kansas public employees retirement

1 system, regents' institutions, or the board of regents.

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

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

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

7 (i) Social security number;

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

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

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

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

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

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

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

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

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

31 ~~Sec. 12.~~ **{13.}** K.S.A. 75-7238 is hereby amended to read as follows:
32 75-7238. (a) There is hereby established the position of executive branch
33 chief information security officer. The CISO shall be in the unclassified
34 service under the Kansas civil service act, shall be appointed by the
35 governor and shall receive compensation in an amount fixed by the
36 governor.

37 (b) The CISO shall:

38 (1) Report to the executive branch chief information technology
39 officer;

40 (2) serve as the state's CISO;

41 (3) serve as the executive branch chief cybersecurity strategist and
42 authority on policies, compliance, procedures, guidance and technologies
43 impacting executive branch cybersecurity programs;

1 (4) ensure Kansas information security office resources assigned or
2 provided to executive branch agencies are in compliance with applicable
3 laws and rules and regulations;

4 (5) coordinate cybersecurity efforts between executive branch
5 agencies;

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

9 (7) *set cybersecurity policy and standards for executive branch*
10 *agencies; and*

11 (8) perform such other functions and duties as provided by law and as
12 directed by the executive chief information technology officer.

13 ~~Sec. 13. {14.}~~ K.S.A. 75-7239 is hereby amended to read as follows:
14 75-7239. (a) There is hereby established within and as a part of the office
15 of information technology services the Kansas information security office.
16 The Kansas information security office shall be administered by the CISO
17 and be staffed appropriately to effect the provisions of the Kansas
18 cybersecurity act.

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

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

31 (1) Administer the Kansas cybersecurity act;

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

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

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

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

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

4 (7) assist in the development of executive branch agency
5 cybersecurity programs ~~that are in~~ *to ensure* compliance with applicable
6 state and federal laws ~~and~~, rules and regulations, *executive branch policies*
7 *and standards and policies* and standards adopted by the information
8 technology executive council;

9 (8) *perform audits of executive branch agencies for compliance with*
10 *applicable state and federal laws, rules and regulations, executive branch*
11 *policies and standards and policies and standards adopted by the*
12 *information technology executive council;*

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

16 ~~(9)~~(10) liaise with external agencies, such as law enforcement and
17 other advisory bodies as necessary, to ensure a strong security posture;

18 ~~(10)~~(11) assist in the development of plans and procedures to manage
19 and recover business-critical services in the event of a cyberattack or other
20 disaster;

21 ~~(11)~~(12) assist executive branch agencies to create a framework for
22 roles and responsibilities relating to information ownership, classification,
23 accountability and protection;

24 ~~(12)~~(13) ensure a cybersecurity ~~training program is provided to~~
25 ~~executive branch agencies at no cost to the agencies~~ *awareness training*
26 *program is made available to all branches of state government;*

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

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

33 ~~(15)~~(14) perform such other functions and duties as provided by law
34 and as directed by the CISO.

35 (d) *Results of audits conducted pursuant to subsection (c)(8) shall be*
36 *confidential and shall not be subject to discovery or disclosure pursuant to*
37 *the open records act, K.S.A. 45-215 et seq., and amendments thereto. The*
38 *provisions of this subsection shall expire on July 1, 2028, unless the*
39 *legislature reviews and acts to continue such provision pursuant to K.S.A.*
40 *45-229, and amendments thereto, prior to July 1, 2028.*

41 Sec. ~~14.~~ **{15.}** K.S.A. 75-7240 is hereby amended to read as follows:
42 75-7240. (a) The executive branch agency heads shall:

43 ~~(a)~~(1) Be solely responsible for security of all data and information

- 1 technology resources under such agency's purview, irrespective of the
2 location of the data or resources. Locations of data may include:
- 3 ~~(1)~~(A) Agency sites;
 - 4 ~~(2)~~(B) agency real property;
 - 5 ~~(3)~~(C) infrastructure in state data centers;
 - 6 ~~(4)~~(D) third-party locations; and
 - 7 ~~(5)~~(E) in transit between locations;
- 8 ~~(b)~~(2) ensure that an agency-wide information security program is in
9 place;
- 10 ~~(e)~~(3) designate an information security officer to administer the
11 agency's information security program that reports directly to executive
12 leadership;
 - 13 ~~(d)~~(4) participate in CISO-sponsored statewide cybersecurity program
14 initiatives and services;
 - 15 ~~(e)~~(5) implement policies and standards to ensure that all the agency's
16 data and information technology resources are maintained in compliance
17 with applicable state and federal laws and rules and regulations;
 - 18 ~~(f)~~(6) implement appropriate cost-effective safeguards to reduce,
19 eliminate or recover from identified threats to data and information
20 technology resources;
 - 21 ~~(g)~~(7) include all appropriate cybersecurity requirements in the
22 agency's request for proposal specifications for procuring data and
23 information technology systems and services;
 - 24 ~~(h)~~ ~~(1)~~(8) (A) submit a cybersecurity—~~assessment~~ *self-assessment*
25 report to the CISO by October 16 of each even-numbered year, including
26 an executive summary of the findings, that assesses the extent to which a
27 ~~computer, a computer program, a computer network, a computer system, a~~
28 ~~printer, an interface to a computer system, including mobile and peripheral~~
29 ~~devices, computer software, or the data processing of the agency or of a~~
30 ~~contractor~~ of the agency is vulnerable to unauthorized access or harm,
31 including the extent to which the agency's or contractor's electronically
32 stored information is vulnerable to alteration, damage, erasure or
33 inappropriate use;
 - 34 ~~(2)~~(B) ensure that the agency conducts annual internal assessments of
35 its security program. Internal assessment results shall be considered
36 confidential and shall not be subject to discovery by or release to any
37 person or agency, outside of the KISO or CISO, *without authorization*
38 *from the executive branch agency director or head*. This provision
39 regarding confidentiality shall expire on July 1, 2023, unless the
40 legislature reviews and reenacts such provision pursuant to K.S.A. 45-229,
41 and amendments thereto, prior to July 1, 2023; and
 - 42 ~~(3)~~(C) prepare or have prepared a—~~summary~~ *financial summary*
43 *identifying cybersecurity expenditures addressing the findings* of the

1 cybersecurity ~~assessment~~ *self-assessment* report required in paragraph (1)
2 *subparagraph (A)*, excluding information that might put the data or
3 information resources of the agency or its contractors at risk and submit
4 such report to the house of representatives committee on ~~government,~~
5 ~~technology and security~~ or its successor committee *appropriations* and the
6 senate committee on ways and means;

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

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

23 (j)(A) Comply with the notification requirements set out in K.S.A.
24 2022 Supp. 50-7a01 et seq., and amendments thereto, and applicable
25 federal laws and rules and regulations, to the same extent as a person who
26 conducts business in this state; and

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

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

32 (1) *Participate in annual agency leadership training to ensure*
33 *understanding of:*

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

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

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

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

43 (2) *ensure that all information technology login credentials are*

1 *disabled the same day that any employee ends their employment with the*
2 *state; and*

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

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

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

20 ~~Sec. 15. {16.}~~ K.S.A. 75-7242 is hereby amended to read as follows:
21 75-7242. Information collected to effectuate this act shall be considered
22 confidential by ~~the executive branch agency and KISO~~ *all state and local*
23 *governmental organizations* unless all data elements or information that
24 specifically identifies a target, vulnerability or weakness that would place
25 the organization at risk have been redacted, including: (a) System
26 information logs; (b) vulnerability reports; (c) risk assessment reports; (d)
27 system security plans; (e) detailed system design plans; (f) network or
28 system diagrams; and (g) audit reports. The provisions of this section shall
29 expire on July 1, 2023, unless the legislature reviews and reenacts this
30 provision pursuant to K.S.A. 45-229, and amendments thereto, prior to
31 July 1, 2023.

32 ~~Sec. 16. {17.}~~ K.S.A. 46-2102, ~~{74-5704,}~~ 75-7201, 75-7202, 75-
33 7205, 75-7206, 75-7208, 75-7209, 75-7210, 75-7211, 75-7237, 75-7238,
34 75-7239, 75-7240 and 75-7242 are hereby repealed.

35 ~~Sec. 17. {18.}~~ This act shall take effect and be in force from and after
36 its publication in the statute book.