

**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~~ **48** hours after the discovery  
20 of 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**

1 **pursuant to K.S.A. 74-5704, and amendments thereto, not later than**  
2 **~~12~~ 48 hours after receipt of such report.**

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

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

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

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

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

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

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

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

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

42 ~~(d)~~*(e)* study the progress and results of all newly implemented  
43 governmental computer hardware and software, information storage,

1 transmission, processing and telecommunications technologies of state  
 2 agencies and institutions including all information technology projects for  
 3 state agencies which have been authorized or for which appropriations  
 4 have been approved by the legislature; and

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

9 **{Sec. 3. K.S.A. 74-5704 is hereby amended to read as follows: 74-  
 10 5704. The committee shall:**

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

14 (b) *adopt rules and regulations that require entities connected to the*  
 15 *Kansas criminal justice information system to report any cybersecurity*  
 16 *incident to the Kansas bureau of investigation not later than ~~12~~ 48 hours*  
 17 *after the discovery of such cybersecurity incident.*}

18 ~~Sec. 3. {4.}~~ K.S.A. 75-7201 is hereby amended to read as follows: 75-  
 19 7201. As used in K.S.A. 75-7201 through 75-7212, and amendments  
 20 thereto:

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

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

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

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

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

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

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

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

17 ~~(e)~~(f) "Joint committee" means the joint committee on information  
18 technology.

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

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

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

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

32 ~~(j)~~(k) "Project start" means the date and time when a state agency  
33 begins a formal study of a business process or technology concept to  
34 assess the needs of the state agency, determines project feasibility or  
35 prepares an information technology project budget estimate under K.S.A.  
36 75-7209, and amendments thereto.

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

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

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

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

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

5 (C) the executive chief information technology officer;

6 (D) the legislative chief information technology officer;

7 (E) the judicial chief information technology officer;

8 (F) the chief executive officer of the state board of regents or such  
9 person's designee;

10 (G) one representative of cities;

11 (H) one representative of counties; the network manager of the  
12 information network of Kansas (INK);

13 (I) one representative with background and knowledge in technology  
14 and cybersecurity from the private sector, ~~however, except that~~ such  
15 representative or such representative's employer shall not be an  
16 information technology or cybersecurity vendor that does business with  
17 the state of Kansas;

18 (J) one representative appointed by the Kansas criminal justice  
19 information system committee;

20 (K) one member of the senate ~~ways and means committee~~ appointed  
21 by the president of the senate or such member's designee;

22 (L) one member of the senate ~~ways and means committee~~ appointed  
23 by the minority leader of the senate or such member's designee;

24 (M) one member of the house ~~government, technology and security~~  
25 ~~committee or its successor committee of representatives~~ appointed by the  
26 speaker of the house of representatives or such member's designee; and

27 (N) one member of the house ~~government, technology and security~~  
28 ~~committee or its successor committee of representatives~~ appointed by the  
29 minority leader of the house of representatives or such member's designee.

30 (2) The chief information technology architect shall be a nonvoting  
31 member of the council.

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

1 ex officio.

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

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

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

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

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

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

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

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

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

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

41 (D) the strategic information technology management plan adopted  
42 by the information technology executive council;

43 (2) report to the chief information technology architect all deviations

1 from the state information architecture that are reported to the executive  
2 information technology officer by executive agencies;

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

9 (4) monitor executive agencies' compliance with:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16 (4) monitor judicial agencies' compliance with:

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

20 (B) the information technology architecture adopted by the  
21 information technology executive council;

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

24 (D) the strategic information technology management plan adopted  
25 by the information technology executive council;

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

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

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

34 ~~Sec. 7.~~ **{8.}** K.S.A. 75-7208 is hereby amended to read as follows: 75-  
35 7208. The legislative chief information technology officer shall:

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

42 (1) ~~The~~ Information technology resource policies and procedures and  
43 project management methodologies adopted by the information technology

1 executive council;

2 (2)~~the~~— information technology architecture adopted by the  
3 information technology executive council;

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

6 (4)~~the~~— strategic information technology management plan adopted by  
7 the information technology executive council;

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

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

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

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

21 (2) ~~the~~— information technology architecture adopted by the  
22 information technology executive council;

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

25 (4) ~~the~~— strategic information technology management plan adopted by  
26 the information technology executive council;

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

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

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

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

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

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

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

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

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

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

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

30 (B) ~~*be consistent with:*~~

31 (i) ~~*Information technology resource policies and procedures and*~~  
32 ~~*project management methodologies for all state agencies;*~~

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

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

37 (iv) ~~*a strategic information technology management plan for the*~~  
38 ~~*state.*~~

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

43 (b) (1) ~~Before one or more state agencies proposing an information~~

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 ~~involving a cost reduction, other than a change in the proposed use of any~~  
2 ~~new or replacement information technology equipment or in the use of any~~  
3 ~~existing information technology equipment that has been significantly~~  
4 ~~upgraded to advise and consult on the status and progress of such~~  
5 ~~information technology project, including revisions to expenditures for the~~  
6 ~~current fiscal year and ensuing fiscal years; and~~

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

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

23 Sec. ~~H.~~ {12.} K.S.A. 75-7237 is hereby amended to read as follows:  
24 75-7237. As used in K.S.A. 75-7236 through 75-7243, and amendments  
25 thereto:

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

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

33 (c) "CISO" means the executive branch chief information security  
34 officer.

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

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

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

43 (g) "Executive branch agency" means any agency in the executive

1 branch of the state of Kansas, but does not include elected office agencies,  
2 the adjutant general's department, the Kansas public employees retirement  
3 system, regents' institutions, or the board of regents.

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

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

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

9 (i) Social security number;

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

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

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

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

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

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

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

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

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

33 ~~Sec. 42.~~ **{13.}** K.S.A. 75-7238 is hereby amended to read as follows:  
34 75-7238. (a) There is hereby established the position of executive branch  
35 chief information security officer. The CISO shall be in the unclassified  
36 service under the Kansas civil service act, shall be appointed by the  
37 governor and shall receive compensation in an amount fixed by the  
38 governor.

39 (b) The CISO shall:

40 (1) Report to the executive branch chief information technology  
41 officer;

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

43 (3) serve as the executive branch chief cybersecurity strategist and

1 authority on policies, compliance, procedures, guidance and technologies  
2 impacting executive branch cybersecurity programs;

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

6 (5) coordinate cybersecurity efforts between executive branch  
7 agencies;

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

11 (7) *set cybersecurity policy and standards for executive branch*  
12 *agencies; and*

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

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

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

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

33 (1) Administer the Kansas cybersecurity act;

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

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

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

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

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

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

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

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

18 ~~(9)~~(10) liaise with external agencies, such as law enforcement and  
19 other advisory bodies as necessary, to ensure a strong security posture;

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

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

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

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

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

35 ~~(15)~~(14) perform such other functions and duties as provided by law  
36 and as directed by the CISO.

37 (d) *Results of audits conducted pursuant to subsection (c)(8) shall be*  
38 *confidential and shall not be subject to discovery or disclosure pursuant to*  
39 *the open records act, K.S.A. 45-215 et seq., and amendments thereto. The*  
40 *provisions of this subsection shall expire on July 1, 2028, unless the*  
41 *legislature reviews and acts to continue such provision pursuant to K.S.A.*  
42 *45-229, and amendments thereto, prior to July 1, 2028.*

43 Sec. ~~14.~~ {15.} K.S.A. 75-7240 is hereby amended to read as follows:

- 1 75-7240. (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 (1)~~  
4 *subparagraph (A)*, excluding information that might put the data or  
5 information resources of the agency or its contractors at risk and submit  
6 such report to the house of representatives committee on ~~government,~~  
7 ~~technology and security~~ or its successor committee *appropriations* and the  
8 senate 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       ~~(H)~~(A) Comply with the notification requirements set out in K.S.A.  
26 2022 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 each state agency 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, 2028,  
20 unless the legislature reviews and reenacts this provision pursuant to  
21 K.S.A. 45-229, and amendments thereto, prior to July 1, 2028.

22 Sec. ~~15.~~ **{16.}** K.S.A. 75-7242 is hereby amended to read as follows:  
23 75-7242. Information collected to effectuate this act shall be considered  
24 confidential by ~~the executive branch agency and KISO~~ all state and local  
25 governmental 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. ~~16.~~ **{17.}** K.S.A. 46-2102, ~~{74-5704,}~~ 75-7201, 75-7202, 75-  
35 7205, 75-7206, 75-7208, 75-7209, 75-7210, 75-7211, 75-7237, 75-7238,  
36 75-7239, 75-7240 and 75-7242 are hereby repealed.

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