



1 parts of acts.

2       Sec. 12c. (1) A covered entity is entitled to an affirmative  
3 defense to any tort cause of action that alleges that the covered  
4 entity's failure to implement reasonable information security  
5 controls resulted in a security breach if the covered entity  
6 demonstrates all of the following, as applicable:

7       (a) The covered entity established, maintained, and reasonably  
8 implemented and complied with a written cybersecurity program that  
9 contains administrative, technical, and physical safeguards for the  
10 protection of personal information and personal identifying  
11 information that reasonably conforms to the current version of an  
12 industry-recognized cybersecurity framework or standard described  
13 in subsection (2) or a combination of the current versions of  
14 industry-recognized cybersecurity frameworks or standards described  
15 in subsection (2).

16       (b) The covered entity's cybersecurity program is designed to  
17 do all of the following:

18       (i) Protect the security and confidentiality of personal  
19 information and personal identifying information.

20       (ii) Protect against anticipated threats or hazards to the  
21 security or integrity of personal information and personal  
22 identifying information.

23       (iii) Protect against unauthorized access to and acquisition of  
24 personal information and personal identifying information that is  
25 likely to result in a material risk of identity theft to the  
26 individual to whom the personal information and personal  
27 identifying information relate.

28       (c) The scale and scope of the covered entity's cybersecurity  
29 program is appropriate based on the factors in subsection (3).



1 (d) Except as otherwise provided in subdivision (e), for its  
2 cybersecurity program under subdivision (a), the covered entity  
3 attained and maintained a third-party certification that is aligned  
4 with the current version of the industry-recognized cybersecurity  
5 framework or standard to which the covered entity's cybersecurity  
6 program reasonably conforms.

7 (e) For a covered entity that is a financial institution and  
8 that does not attain or maintain a third-party certification of its  
9 cybersecurity program as described in subdivision (d), the covered  
10 entity is subject to regular examination or audit by a state or  
11 federal regulatory agency that has oversight over the covered  
12 entity.

13 (2) An industry-recognized cybersecurity framework or standard  
14 means any of the following, as applicable:

15 (a) The Framework for Improving Critical Infrastructure  
16 Cybersecurity developed by the National Institute of Standards and  
17 Technology.

18 (b) The National Institute of Standards and Technology's  
19 Special Publication 800-171.

20 (c) The National Institute of Standards and Technology's  
21 Special Publications 800-53 and 800-53a.

22 (d) The Federal Risk and Authorization Management Program  
23 Security Assessment Framework.

24 (e) The Center for Internet Security Critical Security  
25 Controls for Effective Cyber Defense.

26 (f) The International Organization for  
27 Standardization/International Electrotechnical Commission 27000  
28 Family Information Security Management Systems.

29 (g) If the covered entity is regulated by this state, the



1 federal government, or both, or is otherwise subject to any of the  
2 laws or regulations listed in this subdivision, any of the  
3 following, as applicable:

4 (i) The security requirements under the health insurance  
5 portability and accountability act of 1996, Public Law 104-191, or  
6 the regulations promulgated under that act, 45 CFR parts 160 and  
7 164.

8 (ii) Title V of the Gramm-Leach-Bliley act, 15 USC 6801 to  
9 6827.

10 (iii) The federal information security modernization act of  
11 2014, Public Law 113-283.

12 (iv) The Federal Financial Institutions Examination Council's  
13 Information Security Standards.

14 (h) The Payment Card Industry Data Security Standard.

15 (i) The Information Systems Audit and Control Association's  
16 Control Objectives for Information Related Technology.

17 (3) A covered entity's cybersecurity program is appropriate if  
18 it is based on all of the following factors:

19 (a) The size and complexity of the covered entity.

20 (b) The nature and scope of the activities of the covered  
21 entity.

22 (c) The sensitivity of the information to be protected.

23 (d) The cost and availability of tools to improve information  
24 security and reduce vulnerabilities.

25 (e) The resources available to the covered entity.

26 (4) When a final revision to an industry-recognized  
27 cybersecurity framework or standard listed in subsection (2) is  
28 published or when an industry-recognized cybersecurity framework or  
29 standard under subsection (2) is amended, a covered entity whose



1 cybersecurity program reasonably conforms to that framework or  
2 standard shall reasonably conform to the revised or amended  
3 framework or standard not later than 1 year after the publication  
4 date of the revision or amendment.

5 (5) This section does not provide a private right of action,  
6 including a class action, with respect to any act or practice under  
7 this section.

8 (6) It is the strong policy of this state to apply the laws of  
9 this state to entities that do business in this state in order to  
10 incentivize conformance to a recognized cybersecurity standard or  
11 framework.

12 (7) If there is a choice of law provision in an agreement that  
13 designates this state as the governing law, this section must be  
14 applied, if applicable, to the fullest extent possible in a civil  
15 action brought against a person regardless of whether the civil  
16 action is brought in this state or another state.

17 (8) As used in this section, "covered entity" means a person  
18 that accesses, maintains, communicates, or processes personal  
19 information or personal identifying information in or through 1 or  
20 more systems, networks, or services located in or outside of this  
21 state.

