Utah Code Ann. § 78B-4-703

Current through May 1, 2024 of the 2024 General Session.

Utah Code Annotated > Title 78B Judicial Code (§§ 78B-1-101 — 78B-25-115) > Chapter 4 Limitations on Liability (Pts. 1 — 7) > Part 7 Cybersecurity Affirmative Defense Act (§§ 78B-4-701 — 78B-4-706)

78B-4-703. Components of a cybersecurity program eligible for an affirmative defense.

(1) Subject to Subsection (3), a person's written cybersecurity program reasonably conforms to a recognized cybersecurity framework if the written cybersecurity program:

(a) is designed to protect the type of personal information obtained in the breach of system security; and

(b)

(i) is a reasonable security program described in Subsection (2);

(ii) reasonably conforms to the current version of any of the following frameworks or publications, or any combination of the following frameworks or publications:

(A) NIST special publication 800-171;

(B) NIST special publications 800-53 and 800-53a;

(C) the Federal Risk and Authorization Management Program Security Assessment Framework;

(D) the Center for Internet Security Critical Security Controls for Effective Cyber Defense; or

(E) the International Organization for Standardization/International Electrotechnical Commission 27000 Family - Information security management systems;

(iii) for personal information obtained in the breach of the system security that is regulated by the federal government or state government, reasonably complies with the requirements of the regulation, including:

(A) the security requirements of the Health Insurance Portability and Accountability Act of 1996, as described in 45 C.F.R. Part 164, Subpart C;

(B) Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended;

(C) the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283;

(D) the Health Information Technology for Economic and Clinical Health Act, as provided in 45 C.F.R. Part 164;

(E) Title 13, Chapter 44, Protection of Personal Information Act; or

(F) any other applicable federal or state regulation; or

(iv) for personal information obtained in the breach of system security that is the type of information intended to be protected by the PCI data security standard, reasonably complies with the current version of the PCI data security standard.

(2) A written cybersecurity program is a reasonable security program under Subsection (1)(b)(i) if:

(a) the person coordinates, or designates an employee of the person to coordinate, a program that provides the administrative, technical, and physical safeguards described in Subsections 78B-4-702(4)(a) and (c);

(b) the program under Subsection (2)(a) has practices and procedures to detect, prevent, and respond to a breach of system security;

(c) the person, or an employee of the person, trains, and manages employees in the practices and procedures under Subsection (2)(b);

(d) the person, or an employee of the person, conducts risk assessments to test and monitor the practice and procedures under Subsection (2)(b), including risk assessments on:

(i) the network and software design for the person;

(ii) information processing, transmission, and storage of personal information; and

(iii) the storage and disposal of personal information; and

(e) the person adjusts the practices and procedures under Subsection (2)(b) in light of changes or new circumstances needed to protect the security, confidentiality, and integrity of personal information.

(3)

(a) If a recognized cybersecurity framework described in Subsection (1)(b)(ii) or (iv) is revised, a person with a written cybersecurity program that relies upon that recognized cybersecurity framework shall reasonably conform to the revised version of the framework no later than one year after the day in which the revised version of the framework is published.

(b) If a recognized cybersecurity framework described in Subsection (1)(b)(iii) is amended, a person with a written cybersecurity program that relies upon that recognized cybersecurity framework shall reasonably conform to the amended regulation of the framework in a reasonable amount of time, taking into consideration the urgency of the amendment in terms of:

(i) risks to the security of personal information;

(ii) the cost and effort of complying with the amended regulation; and

(iii) any other relevant factor.

History

2021 ch. 40, § 3, effective May 5, 2021.

End of Document