ORC Ann. 3965.02

Current through File 21 of the 135th General Assembly (2023-2024).

Page's Ohio Revised Code Annotated > Title 39: Insurance (Chs. 3901 — 3999) > Chapter 3965 Cybersecurity framework. (§§ 3965.01 — 3965.11)

§ 3965.02 Licensee to maintain written information security program.

(A) Each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment. The program shall be commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control.

(B) The information security program shall contain administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system and shall be designed to do all of the following:

(1) Protect the security and confidentiality of nonpublic information and the security of the information system;

(2) Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;

(3) Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer;

(4) Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

(C) The licensee shall do all of the following:

(1) Designate one or more persons or entities to act on behalf of the licensee and be responsible for the information security program;

(2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including threats to the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers;

(3) Assess the likelihood and potential damage of the threats described in division (C)(2) of this section, taking into consideration the sensitivity of the nonpublic information;

(4) Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage the threats described in division (C)(2) of this section, including

consideration of such threats in each relevant area of the licensee's operations, including all of the following:

(a) Employee training and management;

(b) Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal;

(c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

(5) Implement information safeguards to manage the threats identified in its ongoing assessment;

(6) Not less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

(D) Based on its risk assessment, the licensee shall do all of the following:

(1) Design its information security program to mitigate the identified risks in a way that is commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control;

(2) Determine which of the following security measures are appropriate and implement such security measures:

(a) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals, to protect against the unauthorized acquisition of nonpublic information;

(b) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;

(c) Restrict access at physical locations containing nonpublic information to authorized individuals;

(d) Protect by encryption or other appropriate means all nonpublic information while such information is being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media;

(e) Adopt secure development practices for in-house developed applications utilized by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee;

(f) Modify the information system in accordance with the licensee's information security program;

(g) Utilize effective controls, which may include multifactor authentication procedures for accessing nonpublic information;

(h) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(i) Include audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

(j) Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures;

(k) Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format.

(3) Include cybersecurity risks in the licensee's enterprise risk management process;

(4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared;

(5) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

(E) If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum, do all of the following:

(1) Require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program;

(2) Require the licensee's executive management or its delegates to report in writing at least annually, all of the following information:

(a) The overall status of the information security program and the licensee's compliance with this chapter;

(b) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in the information security program.

(3) If executive management delegates any of its responsibilities under this section, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegates and shall require the delegates to submit a report that complies with the requirements of division (E)(2) of this section.

(F)

(1) A licensee shall exercise due diligence in selecting its third-party service provider.

(2) A licensee shall require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

(G) The licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with all of the following:

(1) Any relevant changes in technology;

(2) The sensitivity of its nonpublic information;

(3) Internal or external threats to information;

(4) The licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(H)

(1) As part of its information security program, each licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations.

(2) The incident response plan described in division (H) (1) of this section shall address all of the following areas:

(a) The internal process for responding to a cybersecurity event;

(b) The goals of the incident response plan;

(c) The definition of clear roles, responsibilities, and levels of decision-making authority;

(d) External and internal communications and information sharing;

(e) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(f) Documentation and reporting regarding cybersecurity events and related incident response activities;

(g) The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

(I)

(1) By the fifteenth day of February of each year, unless otherwise permitted to file on the first day of June in division (I)(2) of this section, each insurer domiciled in this state shall submit to the superintendent of insurance a written statement certifying that the insurer is in compliance with the requirements set forth in this section. Each insurer shall maintain for examination by the department of insurance all records, schedules, and data supporting this certificate for a period of five years. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems, or processes. Such documentation must be available for inspection by the superintendent.

(2) Notwithstanding division (I)(1) of this section, an insurer domiciled in this state and licensed exclusively to conduct business in this state and no other state shall be permitted to submit to the superintendent of insurance a written statement certifying that the insurer is in compliance with the requirements set forth in this section as part of the insurer's corporate governance annual disclosure required by section 3901.073 of the Revised Code.

(J) A licensee that meets the requirements of this chapter shall be deemed to have implemented a cybersecurity program that reasonably conforms to an industry-recognized cybersecurity framework for the purposes of Chapter 1354. of the Revised Code.

History

2018 sb273, § 1, effective March 20, 2019.

End of Document