N.D. Cent. Code, § 26.1-02.2-03

Current through all legislation from the 68th Legislative Assembly - Special Session (2023).

North Dakota Century Code Annotated > TITLE 26.1 Insurance (Chs. 26.1-01 — 26.1-59) > CHAPTER 26.1-02.2 Insurance Data Security (§§ 26.1-02.2-01 — 26.1-02.2-11)

26.1-02.2-03. Information security program.

1. Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including the licensee's 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, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

2. A licensee's information security program must be designed to:

a. Protect the security and confidentiality of nonpublic information and the security of the information system;

b. Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;

c. Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer; and

d. Define and periodically re-evaluate a schedule for retention of nonpublic information and a mechanism for destruction if no longer needed.

3. The licensee shall:

a. Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee which is responsible for the information security program;

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

c. Assess the likelihood and potential damage of any threats, taking into consideration the sensitivity of the nonpublic information;

d. Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage any threats, including consideration of threats in each relevant area of the licensee's operations, including:

(1) Employee training and management;

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

(3) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

e. Implement information safeguards to manage the threats identified in the licensee's ongoing assessment and assess the effectiveness of the safeguards' key controls, systems, and procedures on an annual basis.

4. Based on the licensee's risk assessment, the licensee shall:

a. Design the information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including the licensee's 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. Determine which security measures as provided under this subdivision are appropriate and implement the security measures:

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

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

(3) Restrict physical access to nonpublic information only to an authorized individual;

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

(5) Adopt secure development practices for in-house developed applications utilized by the licensee;

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

(7) Utilize effective controls, which may include multi-factor authentication procedures for employees accessing nonpublic information;

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

(9) 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;

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

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

c. Include cybersecurity risks in the licensee's enterprise risk management process.

d. Stay informed regarding emerging threats or vulnerabilities and use reasonable security measures if sharing information relative to the character of the sharing and the type of information shared.

e. Provide cybersecurity awareness training to the licensee's personnel which is updated as necessary to reflect risks identified by the licensee in the risk assessment.

5. If the licensee has a board of directors, the board or an appropriate committee of the board at a minimum shall:

a. Require the licensee's executive management or the licensee's delegates to develop, implement, and maintain the licensee's information security program.

b. Require the licensee's executive management or the licensee's delegates to report the following information in writing on an annual basis:

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

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

c. If executive management delegates any responsibilities under this section, the executive management delegates shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegate and shall receive a report from the delegate complying with the requirements of the report to the board of directors.

6. A licensee shall exercise due diligence in selecting its third-party service provider; and 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 accessible to, or held by, the third-party service provider.

7. The licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements, including mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

8. As part of the licensee's information security program, a 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 the licensee's possession. The incident response plan must include the licensee's plan to recover the licensee's information systems and restore continuous functionality of any aspect of the licensee's business or operations.

9. A licensee's incident response plan must address:

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

(2) The goals of the incident response plan;

(3) The definition of clear roles, responsibilities, and levels of decisionmaking authority;

(4) External and internal communications and information sharing;

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

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

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

10. Annually, an insurer domiciled in this state shall submit to the commissioner, a written statement by April fifteenth, certifying the insurer is in compliance with the requirements set forth in this section. An insurer shall maintain for examination by the department 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 the areas, systems, or processes. The documentation must be available for inspection by the commissioner.

History

S.L. 2021, ch. 229, § 1, effective August 1, 2021.