Wis. Stat. § 601.952

This document is current through Act 142 of the 2023-2024 Legislative Session

LexisNexis® Wisconsin Annotated Statutes > Insurance (Chs. 600 — 655) > Chapter 601. Insurance — Administration (Subchs. I — IX) > Subchapter IX Insurance Data Security (§§ 601.95 — 601.956)

601.952. Information security program.

(1) Implementation of program. No later than one year after the effective date of this subsection.... [LRB inserts date], a licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment under sub. (2) and consistent with the conditions of sub. (3) (a). The program shall contain administrative, technical, and physical safeguards for the protection of the licensee's information systems and nonpublic information. The licensee shall design the program to do all of the following:

(a) Protect against threats and hazards to the security and integrity of the information systems and nonpublic information.

(b) Protect against unauthorized access to and use of nonpublic information and minimize the likelihood of harm to a consumer from the unauthorized access or use.

(c) Establish and periodically reevaluate a schedule for retention and disposal of nonpublic information and establish a mechanism for the destruction of nonpublic information that is no longer needed.

(2) Risk assessment. The licensee shall conduct a risk assessment under which the licensee shall do all of the following:

(a) Identify reasonably foreseeable internal and external threats that could result in unauthorized access to or transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including nonpublic information that is accessible to or held by 3rd-party service providers of the licensee.

(b) Assess the likelihood and potential damage of the threats identified under par. (a), taking into consideration the sensitivity of the nonpublic information.

(c) Assess the sufficiency of policies, procedures, information systems, and other safeguards to manage the threats identified under par. (a) in each relevant area of the licensee's operations, including all of the following:

1. Employee training and management.

2. Information systems, including the classification, governance, processing, storage, transmission, and disposal of information.

3. Processes for detecting, preventing, and responding to attacks, intrusions, and other system failures.

(3) Risk management. Based on the risk assessment under sub. (2), the licensee shall do all of the following:

(a) Design an information security program to mitigate the identified threats, commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of 3rd-party service providers, and the sensitivity of the nonpublic information.

(b) Implement the following security measures, as appropriate:

1. Place access controls on information systems.

2. Identify and manage the data, personnel, devices, systems, and facilities that enable the licensee to achieve its business purposes, taking into consideration the relative importance of the data, personnel, devices, systems, and facilities to the business objectives and risk strategy of the licensee.

3. Restrict physical access to nonpublic information to authorized individuals only.

4. Protect, by encryption or other means, nonpublic information being transmitted over an external network and nonpublic information stored on a portable computer or storage device or media.

5. Adopt secure development practices for applications that are developed in-house and utilized by the licensee.

6. Modify information systems in accordance with the licensee's information security program.

7. Utilize effective controls, which may include multifactor authentication procedures for employees accessing nonpublic information.

8. Implement regular testing and monitoring of systems and procedures to detect actual and attempted attacks on, or intrusions into, an information system.

9. Include audit trails within the information security program that are designed to detect and respond to cybersecurity events and to reconstruct material financial transactions sufficient to support the normal operations and obligations of the licensee.

10. Implement measures to protect against the destruction, loss, or damage of nonpublic information due to environmental hazards, natural and other disasters, and technological failures.

11. Develop, implement, and maintain practices for the secure disposal of nonpublic information in all formats.

(c) Designate at least one employee, affiliate, or outside vendor as responsible for the information security program.

(d) Stay informed regarding emerging threats and vulnerabilities and implement safeguards to manage the threats and vulnerabilities.

(e) No less than annually, assess the effectiveness of security safeguards, including key controls, systems, and procedures.

(f) Include cybersecurity risks in the licensee's enterprise risk management process.

(g) Utilize reasonable security measures when sharing information, taking into consideration the character of the sharing and the type of information shared.

(h) Provide personnel with cybersecurity awareness training that is updated as necessary.

(4) Program adjustments. The licensee shall monitor, evaluate, and adjust the information security program under sub. (1) consistent with changes in technology, the sensitivity of the nonpublic information, internal and external threats to nonpublic information, and changes to the licensee's business operations, outsourcing arrangements, and information systems. If a licensee identifies areas, systems, or processes that require material improvement, updating, or redesign, the licensee shall document the identification and remedial efforts to address the areas, systems, or processes. The licensee shall maintain the documentation for a period of at least 5 years starting from the date the documentation was created and shall produce the documentation upon demand of the commissioner.

(5) Incident response plan. As part of its information security program, a licensee shall develop an incident response plan to promptly respond to, and recover from, a cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations. The incident response plan shall be in writing and address all of the following:

(a) The goals of the incident response plan.

(b) The internal process for responding to a cybersecurity event.

(c) The identification of clear roles, responsibilities, and levels of decision-making authority during and immediately following a cybersecurity event.

(d) The external and internal communications and information sharing during and immediately following a cybersecurity event.

(e) Requirements for the remediation of identified weaknesses in the information systems and associated controls.

(f) The reporting and documentation of a cybersecurity event and related incident response activities.

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

(6) Oversight of 3rd-party service provider arrangements. If applicable, no later than 2 years after the effective date of this subsection.... [LRB inserts date], a licensee shall exercise due diligence when selecting any 3rd-party service provider. The licensee shall make reasonable efforts to require a 3rd-party service provider to do all of the following:

(a) 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 3rd-party service provider.

(b) Report a cybersecurity event under s. 601.954.

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

(a) Require the licensee's executive management to develop, implement, and maintain the information security program under sub. (1).

(b) Oversee the development, implementation, and maintenance of the information security program.

(c) Require the licensee's executive management to report, at least annually, all of the following information to the board:

1. The overall status of the information security program and the licensee's compliance with this subchapter.

2. Material matters relating to the information security program, including issues relating to risk assessment, risk management and control decisions, 3rd-party service provider arrangements, and security testing.

3. Recommendations for modifications to the information security program.

(8) Annual certification to commissioner. Beginning in the year that is 2 years after the effective date of this subsection.... [LRB inserts date], a licensee who is domiciled in this state shall annually submit, no later than March 1, to the commissioner a written certification that the licensee is in compliance with the requirements of this section. The licensee shall maintain all records, schedules, and data supporting the certification for a period of at least 5 years and shall produce the records, schedules, and data upon demand of the commissioner.

(9) Exemptions.

(a) This section does not apply to a licensee who meets any of the following criteria:

1. Has less than $10,000,000 in year-end total assets.

2. Has less than $5,000,000 in gross annual revenue.

3. Has fewer than 50 employees, including independent contractors, who work at least 30 hours a week for the licensee.

(b) A licensee who ceases to qualify for the exemption under par. (a) shall comply with this section no later than 180 days after the date the licensee ceases to qualify.

History

2021 a. 73, § 5, effective November 1, 2021.

End of Document