La. R.S. § 22:2504

Current through the 2024 First Extraordinary Session and Act 22 of the Second Extraordinary Session. Revisions of the Louisiana State Law Institute now current through all titles received as of February 1, 2024.

§ 22:2504. Information security program

A. A licensee shall develop, implement, and maintain a comprehensive, written information security program which satisfies all of the following criteria:

(1) Is based on the licensee's risk assessment.

(2) Contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(3) Is commensurate with all of the following:

(a) Size and complexity of the licensee.

(b) Nature and scope of the licensee's activities including its use of third-party service providers.

(c) Sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control.

B. A licensee's information security program 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. A licensee shall conduct a risk assessment by doing all of the following:

(1) Designate one or more employees, an affiliate, or an outside vendor to act on behalf of the licensee and to 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 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 these threats, 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 these threats, including consideration of 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, and, no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

D. Based on the licensee's risk assessment, a licensee shall do all of the following:

(1) Design an 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 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) Implement all of the following security measures that the licensee determines are appropriate:

(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 physical access to nonpublic information to authorized individuals.

(d) 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.

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

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

(g) Use effective controls, which may include multifactor authentication procedures for any individual 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.

(5) Use reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

(6) Provide its personnel with cybersecurity awareness training that reflects current risks identified by the licensee in the risk assessment.

E. If a licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum, require a licensee's executive management or its delegates to do all of the following:

(1) Develop, implement, and maintain the licensee's information security program.

(2) 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 the responsibilities provided for in this Section, management shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegates and shall receive a report from the delegates complying with the requirements of the report to the board of directors above.

F. With regard to third-party service providers, a licensee shall do all of the following:

(1) Exercise due diligence in selecting a third-party service provider.

(2) Require third-party service providers 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. A 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 but not limited to 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 shall address all of the following:

(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 decisionmaking 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 of the incident response plan, as necessary, following a cybersecurity event.

I.

(1) Annually, each insurer domiciled in this state shall submit to the commissioner a written statement by February 15, certifying that the insurer is in compliance with the requirements set forth in R.S. 22:2504.

(2) Each insurer shall maintain for examination by the commissioner all records, schedules, and data supporting the certificate for a period of five years.

(3) To the extent an insurer identifies areas, systems, or processes that require material improvement, update, or redesign, the insurer shall document the identification and the remediation efforts planned and underway to address the areas, systems, or processes. The documentation shall be made available for inspection by the commissioner.

History

Acts 2020, No. 283, § 1, effective August 1, 2020.

End of Document