§2264. Information security program

1. Implementation of information security program. 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 used by the licensee or in the licensee's possession, custody or control, a licensee shall develop, implement and maintain a comprehensive, written information security program based on the licensee's risk assessment and containing administrative, technical and physical safeguards for the protection of nonpublic information and the licensee's information systems.
[PL 2021, c. 24, §1 (NEW).]

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

A. Protect the security and confidentiality of nonpublic information and the security of the licensee's information systems; [PL 2021, c. 24, §1 (NEW).]

B. Protect against reasonably foreseeable threats or hazards to the security or integrity of nonpublic information and the licensee's information systems; [PL 2021, c. 24, §1 (NEW).]

C. Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer; and [PL 2021, c. 24, §1 (NEW).]

D. Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when it is no longer needed. [PL 2021, c. 24, §1 (NEW).]
[PL 2021, c. 24, §1 (NEW).]

3. Risk assessment. A licensee shall:

A. Designate one or more employees, an affiliate or another person to act on behalf of the licensee to be responsible for the licensee's information security program; [PL 2021, c. 24, §1 (NEW).]

B. Identify reasonably foreseeable internal or external threats that could result in unauthorized access to or transmission, disclosure, misuse, alteration or destruction of nonpublic information, including threats to the security of the licensee's information systems and nonpublic information that are accessible to or held by 3rd-party service providers; [PL 2021, c. 24, §1 (NEW).]

C. Assess the likelihood and potential damage of the threats described in paragraph B, taking into consideration the sensitivity of the nonpublic information; [PL 2021, c. 24, §1 (NEW).]

D. Assess the sufficiency of policies, procedures and other safeguards in place to manage the threats described in paragraph B, 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 system failures; and [PL 2021, c. 24, §1 (NEW).]

E. At least annually, assess the effectiveness of the key controls, information systems and procedures and other safeguards in paragraph D implemented to manage the threats described in paragraph B that are identified in the licensee's ongoing assessment. [PL 2021, c. 24, §1 (NEW).]
[PL 2021, c. 24, §1 (NEW).]

4. Risk management. Based on its risk assessment pursuant to subsection 3, a licensee shall:

A. Design its 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 its

use of 3rd-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control; [PL 2021, c. 24, §1 (NEW).]

B. Consider the following security measures and implement the measures considered appropriate:

(1) 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;

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

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

(4) Protect, by encryption or other appropriate means, all nonpublic information while it 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;

(5) Adopt secure development practices for applications developed and used by the licensee and procedures for evaluating, assessing or testing the security of externally developed applications used by the licensee;

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

(7) Use effective controls, which may include multifactor authentication procedures, for individuals 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 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, such as 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; [PL 2021, c. 24, §1 (NEW).]

C. Include cybersecurity risks in the licensee's enterprise risk management process; [PL 2021, c. 24, §1 (NEW).]

D. Stay informed regarding emerging threats to or vulnerabilities of information systems and use reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and [PL 2021, c. 24, §1 (NEW).]

E. Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in its risk assessment. [PL 2021, c. 24, §1 (NEW).]

[PL 2021, c. 24, §1 (NEW).]

5. Oversight by board of directors. If a licensee has a board of directors, the board or an appropriate committee of the board, at a minimum, shall require the licensee's executive management or the executive management's delegates to:

A. Develop, implement and maintain the licensee's information security program; and [PL 2021, c. 24, §1 (NEW).]

B. Report to the board in writing at least annually the following information:

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

(2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, 3rd-party service provider arrangements, results of testing, cybersecurity events or cybersecurity violations and the executive management's responses to cybersecurity events or cybersecurity violations, and recommendations for changes to the information security program. [PL 2021, c. 24, §1 (NEW).]

If a licensee's executive management delegates any of its responsibilities under this section, the licensee's executive management shall oversee each delegate's efforts with respect to the development, implementation and maintenance of the licensee's information security program and shall require each delegate to submit a report to the board pursuant to paragraph B.
[PL 2021, c. 24, §1 (NEW).]

6. Oversight of 3rd-party service provider arrangements. A licensee shall:

A. Exercise due diligence in selecting its 3rd-party service providers; and [PL 2021, c. 24, §1 (NEW).]

B. Require each 3rd-party service provider to implement appropriate administrative, technical and physical safeguards to protect and secure the information systems and nonpublic information that are accessible to or held by the 3rd-party service provider. [PL 2021, c. 24, §1 (NEW).]
[PL 2021, c. 24, §1 (NEW).]

7. Program adjustments. A licensee shall monitor, evaluate and adjust, as appropriate, its information security program consistent with any relevant changes in technology, the sensitivity of the licensee's nonpublic information, internal or external threats to nonpublic information and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.
[PL 2021, c. 24, §1 (NEW).]

8. Incident response plan. As part of its 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 its possession; the licensee's information systems; or the continuing functionality of any aspect of the licensee's business or operations. The incident response plan must address the following areas:

A. The internal process for responding to a cybersecurity event; [PL 2021, c. 24, §1 (NEW).]

B. The goals of the incident response plan; [PL 2021, c. 24, §1 (NEW).]

C. The definition of clear roles, responsibilities and levels of decision-making authority; [PL 2021, c. 24, §1 (NEW).]

D. External and internal communications and information sharing; [PL 2021, c. 24, §1 (NEW).]

E. Requirements for the remediation of any identified weaknesses in the licensee's information systems and associated controls; [PL 2021, c. 24, §1 (NEW).]

F. Documentation and reporting regarding cybersecurity events and related incident response activities; and [PL 2021, c. 24, §1 (NEW).]

G. The evaluation and revision as necessary of the incident response plan following a cybersecurity event. [PL 2021, c. 24, §1 (NEW).]
[PL 2021, c. 24, §1 (NEW).]

9. Annual certification to superintendent. By April 15th annually, an insurance carrier domiciled in this State shall submit to the superintendent a written statement certifying that the insurance carrier is in compliance with the requirements set forth in this section. An insurance carrier shall maintain for examination by the superintendent all records, schedules and data supporting this certification for a period of 5 years. To the extent that an insurance carrier has identified areas, systems or processes that require material improvement, updating or redesign, the insurance carrier shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. The documentation required pursuant to this subsection must be available for inspection by the superintendent.

[PL 2021, c. 24, §1 (NEW).]

SECTION HISTORY

PL 2021, c. 24, §1 (NEW).