215 ILCS 215/10

Statutes current with legislation through P.A. 103-585 of the 2024 Regular Session of the 103rd General Assembly.

Illinois Compiled Statutes Annotated > Chapter 215 INSURANCE (§§ 5/1 — 215/999) > Insurance Data Security Law (§§ 215/1 — 215/999)

215 ILCS 215/10 Information security program.

(a) 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, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(b) A licensee's information security program shall be designed to:

(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;

(4) minimize the likelihood of harm to any consumer; and

(5) define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed, except if the information is otherwise required to be retained by law or rule or if targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

(c) A licensee shall:

(1) designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee who is 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:

(A) employee training and management;

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

(C) detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(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 its risk assessment, the licensee shall:

(1) 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 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) select and implement appropriate security measures from the following:

(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 only 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 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, including 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, including fire and water damage, other catastrophes, or technological failures; and

(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; and

(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:

(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, the following information:

(A) the overall status of the information security program and the licensee's compliance with this Act; and

(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; and

(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 delegate and shall receive a report from the delegate complying with the requirements of the report to the board of directors.

(f) 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 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 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.

(h) 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 shall address the following areas:

(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 decision-making 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 of the incident response plan following a cybersecurity event, as necessary.

(i) Annually, an insurer domiciled in this State shall submit to the Director a written statement by April 15 certifying that the insurer is in compliance with the requirements set forth in this Section. Each insurer shall maintain for examination by the Department all records, schedules, and data supporting this certificate for a period of 5 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. The documentation of identified areas, systems, or processes must be available for inspection by the Director.

(j) Licensees shall comply with subsection (f) 2 years after the effective date of this Act, and shall comply with all other subsections of this Section one year after the effective date of this Act.

History

2023 P.A. 103-142, § 10, effective January 1, 2024.

End of Document