THE INSURANCE CODE OF 1956 (EXCERPT)
Act 218 of 1956

500.555 Comprehensive written information security program; requirements; duties of licensee and board of directors; third-party service provider; incident response plan; certification of compliance.

Sec. 555. (1) 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, 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 do all of the following:

(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.

(d) Maintain policies and procedures for the secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or for other legitimate business purposes.

(3) A licensee shall do all of the following:

(a) Designate 1 or more employees, an affiliate, or an outside vendor to act on behalf of the licensee that 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 that are accessible to, or held by, third-party service providers.

(c) Assess the likelihood and potential damage of these 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 these threats, including consideration of threats in each relevant area of the licensee's operations, including all of the following:

(*i*) Employee training and management.

(*ii*) Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal.

(*iii*) Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

(e) 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.

(4) Based on its risk assessment, a licensee shall do all of the following:

(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 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 of the following security measures are appropriate and implement those appropriate security measures:

(*i*) Placing 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.

(*ii*) Identifying and managing 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.

(*iii*) Restricting physical access to nonpublic information to authorized individuals only.

(*iv*) Protecting 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.

(*v*) Adopting secure development practices for in-house developed applications utilized by the licensee.

(*vi*) Adding procedures for evaluating, assessing, or testing the security of externally developed applications used by the licensee.

(*vii*) Modifying the information system in accordance with the licensee's information security program.

(*viii*) Using effective controls, which may include multi-factor authentication procedures for employees accessing nonpublic information.

(*ix*) Regularly testing and monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems.

(*x*) Including 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.

(*xi*) Implementing 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.

(*xii*) Developing, implementing, and maintaining 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 utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

(e) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

(5) 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 or its delegates to develop, implement, and maintain the licensee's information security program.

(b) Require the licensee's executive management or its delegates to report in writing, at least annually, all of the following information:

(*i*) The overall status of the information security program and the licensee's compliance with this chapter.

(*ii*) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, results of testing, cybersecurity events or violations, and management's responses to the material matters described in this subparagraph, and recommendations for changes in the information security program.

(*iii*) 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 a 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. 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.

(7) 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, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(8) 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. An incident response plan under this subsection must address all of the following areas:

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

(9) By February 15 of each year, each insurer domiciled in this state shall submit to the director a written statement, certifying that the insurer is in compliance with the requirements of this section. Each insurer shall maintain for examination by the department all records, schedules, and data supporting this certificate for 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 the areas, systems, or processes. The documentation described in this subsection must be available for inspection by the director.

History: Add. 2018, Act 690, Eff. Jan. 20, 2021.

Popular name: Act 218