S.C. Code Ann. § 38-99-20

This document is current through 2024 Regular Session Act No. 120, not including changes and corrections made by the Code Commissioner.

South Carolina Code of Laws Annotated by LexisNexis® > Title 38. Insurance (Chs. 1 — 101) > Chapter 99. South Carolina Insurance Data Security Act (§§ 38-99-10 — 38-99-100)

§ 38-99-20. 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 must be designed to:

(1) protect the security and confidentiality of nonpublic information and the security of the information system;

(2) protect against 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 a consumer; and

(4) define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

(C) The licensee shall:

(1) designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee as responsible for the information security program;

(2) identify reasonably foreseeable internal or external threats that could result in the unauthorized access to or 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, considering the sensitivity of the nonpublic information;

(4) assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, taking into consideration threats in each relevant area of the licensee's operations, including:

(a) employee training and management;

(b) information systems, including network and software design, and 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 at least 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'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) determine the appropriateness of and implement the following security measures:

(a) 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;

(b) 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;

(c) restricting access at physical locations containing nonpublic information to authorized individuals;

(d) 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;

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

(f) modifying the information system in accordance with the licensee's information security program;

(g) utilizing effective controls, which may include multifactor authentication procedures for an individual accessing nonpublic information;

(h) regularly testing and monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(i) 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;

(j) 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; and

(k) developing, implementing, and maintaining 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 use reasonable security measures when sharing information relative to the character of the sharing and the type of information shared;

(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)

(1) If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(a) require the licensee's executive management or its delegates to develop, implement, and maintain the licensee's information security program; and

(b) require the licensee's executive management or its delegates to report in writing at least annually:

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

(ii) material matters related to the information security program addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, testing results, cybersecurity events or violations and management's responses, and recommendations for changes in the information security program.

(2) If the executive management of a licensee delegates any of its responsibilities under this chapter, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegates and receive a report from the delegates which must comply with the requirements of the report to the board of directors.

(F) A licensee shall:

(1) exercise due diligence in selecting its third-party service provider; and

(2) 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 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, a licensee must establish a written incident response plan designed to promptly respond to, and recover from, a 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) An incident response plan required in item (1) must address:

(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; and

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

(I) Annually, each insurer domiciled in this State shall submit to the director, a written statement by February fifteenth, 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 five 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. Such documentation must be available for inspection by the director.

History

2018 Act No. 171, § 3, effective January 1, 2019.