Va. Code Ann. § 38.2-623

Current through 2024 Acts effective April 1, 2024

Code of Virginia 1950 > Title 38.2. Insurance. (Chs. 1 — 66) > Chapter 6. Insurance Information and Privacy Protection. (Arts. 1 — 2) > Article 2. Insurance Data Security Act. (§§ 38.2-621 — 38.2-629)

§ 38.2-623. 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 assessment of the licensee's risk and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

B. Each 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 reasonably foreseeable 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; and

4. Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction.

C. Each 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. 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;

3. Place access controls on information systems, including controls to authenticate and permit access only to authorized persons to protect against the unauthorized acquisition of nonpublic information;

4. At physical locations containing nonpublic information, restrict access to nonpublic information to authorized persons only;

5. 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;

6. Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format;

7. 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

8. Provide its personnel with cybersecurity awareness training.

D.

1. If a licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum, require the licensee's information executive management or its delegates to (i) develop, implement, and maintain the licensee's information security program and (ii) report in writing (a) the overall status of the information security program and the licensee's compliance with this article 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.

2. 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 subdivision 1.

E. Beginning July 1, 2022, if a licensee utilizes a third-party service provider, the 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.

F. Each 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.

G. 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. Such incident response plan shall address:

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

H. Beginning in 2023 and annually thereafter, each insurer domiciled in the Commonwealth shall, by February 15, submit to the Commissioner a written statement certifying that the insurer is in compliance with the requirements set forth in this section, any rules adopted pursuant to this article, and any requirements prescribed by the Commission. Each insurer shall maintain for examination by the Bureau 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 Commissioner.

History

2020, c. 264.