Md. Insurance Code Ann. § 33-103

Current through all legislation from the 2023 Regular Session of the General Assembly.

Michie's™ Annotated Code of Maryland > Insurance (Titles 1 — 33) > Title 33. Insurance Data Security. (§§ 33-101 — 33-109)

§ 33-103. Information security program — Design of program — Duties of carrier and risk assessment — Actions by board of directors — Measures by third-party service provider — Incident response plan.

(a)

(1) Each carrier shall develop, implement, and maintain a comprehensive written information security program based on the carrier's risk assessment.

(2) The information security program shall contain administrative, technical, and physical safeguards for the protection of nonpublic information and the carrier's information system.

(3) A carrier's information security program shall be commensurate with:

(i) the size and complexity of the carrier;

(ii) the nature and scope of the carrier's activities, including its use of third-party service providers; and

(iii) the sensitivity of the nonpublic information used by the carrier or in the carrier's possession, custody, or control.

(b) A carrier'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 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) Each carrier shall:

(1) designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the carrier 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 the threats described under item (2) of this subsection, 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 the threats described under item (2) of this subsection, including consideration of threats in each relevant area of the carrier's operations, such as:

(i) employee training and management;

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

(iii) detecting, preventing, and responding to attacks, intrusions, or other system failures;

(5) implement information safeguards to manage the threats identified in its ongoing assessment; and

(6) at least annually, assess the effectiveness of the key controls, systems, and procedures of the safeguards.

(d) Based on its risk assessment, a carrier shall:

(1) design its information security program to mitigate the identified risks, commensurate with the size and complexity of the carrier's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the carrier or in the carrier's possession, custody, or control; and

(2) determine which of the following security measures are appropriate and implement the appropriate security measures:

(i) placement of access controls on information systems, including controls to authenticate and allow access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;

(ii) identification and management of 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) restriction of access at physical locations containing nonpublic information to authorized individuals only;

(iv) protection, by encryption or other appropriate means, of all nonpublic information:

1. during transmission over an external network; and

2. stored on a laptop computer or other portable computing or storage device or media;

(v) adoption of secure development practices for in-house developed applications used by the carrier and procedures for evaluating, assessing, or testing the security of externally developed applications used by the carrier;

(vi) modification of the information system in accordance with the carrier's information security program;

(vii) use of effective controls, which may include multifactor authentication procedures for an individual accessing nonpublic information;

(viii) regular testing and monitoring of systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(ix) inclusion of audit trails within the information security program designed to:

1. detect and respond to cybersecurity events; and

2. reconstruct material financial transactions sufficient to support normal operations and obligations of the carrier;

(x) implementation of 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

(xi) development, implementation, and maintenance of procedures for the secure disposal of nonpublic information in any format.

(e) A carrier's enterprise risk management process shall include cybersecurity risks.

(f) Each carrier shall:

(1) 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; and

(2) provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the carrier in the risk assessment.

(g)

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

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

(ii) require the carrier's executive management or its delegates to report in writing, at least annually, the following information:

1. the overall status of the information security program and the carrier's compliance with this title; and

2. 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 of a carrier delegates any of the responsibilities under this section, the executive management shall:

(i) oversee the development, implementation, and maintenance of the carrier's information security program prepared by the delegates; and

(ii) receive a report from the delegates that complies with the requirements for the report to the board of directors under paragraph (1) of this subsection.

(h) A carrier 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.

(i)

(1) Each carrier 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 carrier's information systems, or the continuing functionality of any aspect of the carrier's business or operations.

(2) The incident response plan shall address the following areas:

(i) the internal process for responding to a cybersecurity event;

(ii) the goals of the incident response plan;

(iii) the definition of clear roles, responsibilities, and levels of decision-making authority;

(iv) external and internal communications and information sharing;

(v) identification of requirements for the remediation of identified weaknesses in information systems and associated controls;

(vi) documentation and reporting regarding cybersecurity events and related incident response activities; and

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

(j)

(1) Except as provided in subsection (k) of this section, on or before April 15 each year, each carrier shall submit to the Commissioner a written statement certifying that the carrier is in compliance with the requirements set forth in this section.

(2) Each carrier shall maintain for examination by the Commissioner all records, schedules, and data supporting this certificate for a period of 5 years.

(k) A carrier that is not domiciled in the State is exempt from the provisions of subsection (j)(1) of this section if the carrier:

(1)

(i) is domiciled in another United States insuring jurisdiction that has adopted a law or regulation that is substantially similar to this section;

(ii) is subject to that law or regulation;

(iii) is required to file a certification of compliance with its domestic regulator under that law or regulation; and

(iv) actually files the required certification with its domestic regulator; or

(2)

(i) is a member of an insurance holding company system, as defined in § 7-101 of this article; and

(ii) has implemented and is subject to an information security program that has been approved and is maintained by another carrier within the same insurance holding company system that meets all of the criteria set forth in item (1) of this subsection.

History

2022, ch. 231, § 1.

End of Document