# 18 Del. C. § 8604

This document is current through 84 Del. Laws, c. 254.

*Delaware Code Annotated > Title 18 Insurance Code (Pts. I — II) > Part II Miscellaneous (Chs. 77 — 88) > Chapter 86 Insurance Data Security Act (§§ 8601 — 8611)*

## § 8604. Information security program [For application of this section, see 82 Del. Laws, c. 176, § 2].

**(a) Implementation of an information security program. —**

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

**(2)** An information security program under this section must be commensurate with the size and complexity of a licensee; the nature and scope of a licensee's activities, including the licensee's use of a third-party service provider; and the sensitivity of the nonpublic information that the licensee uses or has in the licensee's possession, custody, or control.

**(b) Objectives of information security program. —** A licensee's information security program must be designed to do all of the following:

**(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.

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

**(c) Risk assessment. —** A licensee shall do all of the following:

**(1)** Designate 1 or more employees, an affiliate, or an outside vendor designated to act on the licensee's behalf and be responsible for managing and overseeing 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 an information system or nonpublic information that a third-party service provider has access to or holds.

**(3)** Assess the likelihood and potential damage of a threat identified under paragraph (c)(2) of this section, 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 a threat identified under paragraph (c)(2) of this section, including consideration of threats in each relevant area of the licensee's operations, including all of the following:

**a.** Employee training and management.

**b.** An information system, including network and software design and information classification, governance, processing, storage, transmission, and disposal.

**c.** Detecting, preventing, and responding to an attack, intrusion, or other system failure.

**(5)** Implement information safeguards to manage the threats identified in the licensee's ongoing assessment under paragraph (c)(2) of this section and, at least annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

**(d) Risk management. —** Based on a licensee's risk assessment, the licensee shall do all of the following:

**(1)** Design an information security program to mitigate the identified risks, commensurate with all of the following:

**a.** The licensee's size and complexity.

**b.** The nature and scope of the licensee's activities, including the licensee's use of a third-party service provider.

**c.** The sensitivity of the nonpublic information that the licensee uses or has in the licensee's possession, custody, or control.

**(2)** Determine if a security measure listed in paragraphs (d)(2)a. through k. of this section is appropriate and implement each appropriate security measure.

**a.** Place an access control on an information system, including a control to authenticate and permit access only to an authorized individual 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 physical access to nonpublic information to authorized individuals only.

**d.** Protect by encryption or other appropriate means all nonpublic information while the nonpublic information is 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 both of the following:

**1.** Secure development practices for an application that a licensee uses and was developed in-house.

**2.** Procedures for evaluating, assessing, or testing the security of an application that a licensee uses and was developed externally.

**f.** Modify the information system in accordance with the licensee's information security program.

**g.** Utilize effective controls, which may include multi-factor authentication procedures for employees or authorized individuals accessing nonpublic information.

**h.** Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions, into an information system.

**i.** Include audit controls within the information security program designed to do both of the following:

**1.** Detect and respond to a cybersecurity event.

**2.** Reconstruct material financial transactions sufficient to support the licensee's normal operations and obligations.

**j.** Implement measures to protect against the destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage, other catastrophes, or technological failures.

**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.

**(5)** Provide the licensee's personnel with cybersecurity awareness training that is updated as necessary to reflect risks that the licensee identified in the licensee's risk assessment under this section.

**(e) Oversight by board of directors. —** 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:

**(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 all of the following information:

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

**b.** Material matters related to the information security program, including addressing issues such as the following:

**1.** Risk assessment, risk management, and control decisions.

**2.** Third-party service provider arrangements.

**3.** Results of testing.

**4.** Cybersecurity events or violations and management's responses to the events.

**5.** Recommendations for changes in the information security program.

**(3)** If executive management delegates any of its responsibilities under this section, all of the following must occur:

**a.** Executive management shall oversee the development, implementation, and maintenance of the licensee's information security program that the delegate prepares.

**b.** The delegate shall submit to executive management a report that complies with the requirements of the report to the board of directors under paragraph (e)(2) of this section.

**(f) Oversight of third-party service provider arrangements. —**

**(1)** A licensee shall exercise due diligence in selecting a third-party service provider.

**(2)** A licensee shall require a third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information system and nonpublic information that the third-party service provider has access to or holds. The third-party service provider is not considered to have access to or hold encrypted nonpublic information for purposes of this section if the associated protective process or key necessary to assign meaning to the nonpublic information is not within the third-party service provider's possession.

**(g) Program adjustments. —** A licensee shall monitor, evaluate, and adjust as appropriate the information security program consistent with all of the following:

**(1)** Relevant changes in technology.

**(2)** The sensitivity of the licensee's nonpublic information.

**(3)** Internal or external threats to information.

**(4)** The licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

**(h) Incident response plan. —**

**(1)** As part of a licensee's information security program, the licensee shall 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 any of the following:

**a.** Nonpublic information in the licensee's possession.

**b.** The licensee's information system.

**c.** The continuing functionality of any aspect of the licensee's business or operations.

**(2)** An incident response plan under this section 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 an information system and associated controls.

**f.** Documentation and reporting regarding cybersecurity events and related incident response activities.

**g.** As necessary, the evaluation and revision of the incident response plan following a cybersecurity event.

**(i) Annual certification to the Commissioner of domiciliary state. —** An insurer domiciled in this State shall do all of the following:

**(1)** Submit annually to the Commissioner a written statement by February 15, certifying that the insurer is in compliance with the requirements under in this section.

**(2)** Maintain for the Department's examination all records, schedules, and data supporting a certificate under this subsection for a period of 5 years.

**(3)** To the extent an insurer has identified an area, system, or process that requires material improvement, updating, or redesign, document the identification and the remedial effort planned and underway to address the identified area, system, or process. Documentation under this paragraph (i)(3) must be available for the Commissioner's inspection.

## History

82 Del. Laws, c. 176, § 1.



End of Document