40 Pa.C.S. § 4513

Pa.C.S. documents are current through 2024 Regular Session Act 13; P.S. documents are current through 2024 Regular Session Act 13

§ 4513. Information security program.

(a) Requirement for implementation and objectives. Each licensee shall develop, implement and maintain a comprehensive written information security program based on the licensee's risk assessment that:

(1) Contains administrative, technical and physical safeguards for the protection of nonpublic information and the licensee's information systems.

(2) Is commensurate with the following:

(i) The size and complexity of the licensee.

(ii) The nature and scope of the licensee's activities, including the licensee's use of third-party service providers.

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

(3) Is designed to protect:

(i) The security and confidentiality of nonpublic information and the security of the information systems.

(ii) Against any threats or hazards to the security or integrity of nonpublic information and the information systems.

(iii) Against unauthorized access to or use of nonpublic information and that minimizes the likelihood of harm to a consumer.

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

(b) Designation of responsibility. A licensee shall designate one or more employees, an affiliate or an outside vendor to act on behalf of the licensee who shall be responsible for the information security program of the licensee.

(c) Standards. A licensee shall develop an information security program based on its risk assessment and shall:

(1) Design its information security program to mitigate the identified risks, in a manner that is commensurate with the following:

(i) The size and complexity of the licensee.

(ii) The nature and scope of the licensee's activities, including the licensee's use of third-party service providers.

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

(2) Determine which security measures are appropriate and implement the security measures by:

(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 licensee to achieve business purposes in accordance with their relative importance to business objectives and the licensee's risk strategy.

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

(iv) Protecting, by encryption or other appropriate means, all nonpublic information 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) Modifying the information systems in accordance with the licensee's information security program.

(vii) Utilizing effective controls, which may include multifactor authentication procedures, for any employees accessing nonpublic information.

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

(ix) 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.

(x) 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.

(xi) 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 utilize 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.

(d) Monitoring, evaluation and adjustment. A licensee shall monitor, evaluate and adjust, as appropriate, the information security program consistent with:

(1) Any 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.

(e) Incident response plan. As part of its information security program, each licensee shall establish and maintain 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. The incident response plan shall address the following areas:

(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.

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

History

Act 2023-2 (H.B. 739), § 1, approved June 14, 2023, effective December 11, 2023.