Burns Ind. Code Ann. § 27-2-27-18

Current through P.L. 4-2024 of the Second Regular Session of the 123rd General Assembly.

Burns' Indiana Statutes Annotated > Title 27 Insurance (Arts. 1 — 19) > Article 2 Powers and Duties of Insurers (Chs. 1 — 29) > Chapter 27 Insurance Data Security (§§ 27-2-27-1 — 27-2-27-32)

27-2-27-18. Licensee's duties after risk assessment.

Based on the results of the risk assessment, a licensee shall do the following:

(1) Design its information security program to mitigate the identified risks, commensurate with:

(A) the licensee's size and complexity;

(B) the nature and scope of the licensee's activities; and

(C) the sensitivity of the nonpublic information in the licensee's control.

(2) Determine and implement appropriate security measures, which may include the following:

(A) Placing access controls on information systems, including controls to authenticate and permit only authorized individuals to have access to nonpublic information.

(B) 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 risk strategy.

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

(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.

(F) Modifying information systems in accordance with the licensee's information security program.

(G) Using effective controls, which may include multi-factor authentication procedures for any employees 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 a cybersecurity event 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.

(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.

(5) Use reasonable security measures when sharing information, relative to the character of the sharing and the type of information shared.

(6) Provide personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified in the risk assessment.

History

P.L.130-2020, § 10, effective July 1, 2020.