HRS § 431:3B-203

[§ 431: 3B-203.] Risk management.

Based on its risk assessment, the licensee shall:

(1) Design its information security program to mitigate the identified risks, commensurate with the size and complexity 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;

(2) Determine which security measures listed in this paragraph are appropriate and implement those security measures:

(A) Place 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;

(B) Identify and manage 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;

(C) Restrict access at physical locations containing nonpublic information only to authorized individuals;

(D) Protect 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) Adopt secure development practices for in-house developed applications used by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications used by the licensee;

(F) Modify the information system in accordance with the licensee's information security program;

(G) Use effective controls, which may include multi-factor authentication procedures for any individual accessing nonpublic information;

(H) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(I) Include audit trails within the information security program designed to detect and respond to cybersecurity events and reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

(J) 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; and

(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 use reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

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

History

L 2021, c 112, § 2, effective July 1, 2021.

End of Document