60A.9851 INFORMATION SECURITY PROGRAM.

Subdivision 1. **Implementation of an information security program.** Commensurate with the size and complexity of the licensee, the nature and scope 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, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

Subd. 2. **Objectives of an information security program.** A licensee'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 any 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 any consumer; and

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

Subd. 3. **Risk assessment.** The licensee shall:

(1) designate one or more employees, an affiliate, or an outside vendor authorized to act on behalf of the licensee 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 threats to 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 identified pursuant to clause (2), 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 these threats, including consideration of threats in each relevant area of the licensee's operations, including:

(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 systems failures; and

(5) implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.

Subd. 4. **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, the nature and scope 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 of the following security measures are appropriate and implement any appropriate security measures:

(i) 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;

(ii) 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;

(iii) restrict physical access to nonpublic information to authorized individuals only;

(iv) 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;

(v) adopt secure development practices for in-house developed applications utilized by the licensee;

(vi) modify the information system in accordance with the licensee's information security program;

(vii) utilize effective controls, which may include multifactor authentication procedures for any authorized individual accessing nonpublic information;

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

(ix) include 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) implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage, other catastrophes, or technological failures; and

(xi) 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; 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.

Subd. 5. **Oversight by board of directors.** If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(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, the following information:

(i) the overall status of the information security program and the licensee's compliance with sections 60A.985 to 60A.9858; and

(ii) 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; and

(3) if executive management delegates any of its responsibilities under this section, it shall oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegate and shall receive a report from the delegate complying with the requirements of the report to the board of directors.

Subd. 6. **Oversight of third-party service provider arrangements.** (a) A licensee shall exercise due diligence in selecting its third-party service provider.

(b) A licensee 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.

Subd. 7. **Program adjustments.** The licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

Subd. 8. **Incident response plan.** (a) As part of its information security program, each licensee 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 licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations.

(b) 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; and

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

Subd. 9. **Annual certification to commissioner.** (a) Subject to paragraph (b), by April 15 of each year, an insurer domiciled in this state shall certify in writing to the commissioner that the insurer is in compliance with the requirements set forth in this section. Each insurer shall maintain all records, schedules, and data supporting this certificate for a period of five years and shall permit examination by the commissioner. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems, or processes. Such documentation must be available for inspection by the commissioner.

(b) The commissioner must post on the department's website, no later than 60 days prior to the certification required by paragraph (a), the form and manner of submission required and any instructions necessary to prepare the certification.

History: *1Sp2021 c 4 art 3 s 6*