507F.4 Information security program.

1. *a.* Commensurate with the size and complexity of a licensee, the nature and scope of a licensee's activities including the licensee's use of third-party service providers, and the sensitivity of nonpublic information used by the licensee or that is in the licensee's possession, custody, or control, the licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment conducted pursuant to subsection 3.

b. This section shall not apply to any of the following:

(1) A licensee that meets any of the following criteria:

(a) Has fewer than twenty individuals on its workforce, including employees and independent contractors.

(b) Has less than five million dollars in gross annual revenue.

(c) Has less than ten million dollars in year-end total assets.

(2) An employee, agent, representative, or designee of a licensee, and the employee, agent, representative, or designee is also a licensee, if the employee, agent, representative, or designee is covered by the information security program of the other licensee.

c. A licensee shall have one hundred eighty calendar days from the date the licensee no longer qualifies for exemption under paragraph *"b"* to comply with this section.

2. A licensee's information security program must be designed to do all of the following:

a. Protect the security and confidentiality of nonpublic information and the security of the licensee's information system.

b. Protect against threats or hazards to the security or integrity of nonpublic information and the licensee's information system.

c. Protect against unauthorized access to or the use of nonpublic information, and minimize the likelihood of harm to any consumer.

d. Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for the destruction of nonpublic information if retention is no longer necessary for the licensee's business operations, or is no longer required by applicable law.

3. A licensee shall conduct a risk assessment that accomplishes all of the following:

a. Designates one or more employees, an affiliate, or an outside vendor to act on behalf of the licensee and that has responsibility for the information security program.

b. Identifies reasonably foreseeable internal or external threats that may result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including nonpublic information that is accessible to, or held by, a third-party service provider.

c. Assesses the probability of, and the potential damage caused by, the threats identified in paragraph *"b"*, taking into consideration the sensitivity of nonpublic information.

d. Assesses the sufficiency of policies, procedures, information systems, and other safeguards in place to manage the threats identified in paragraph *"b"*. This assessment must include consideration of threats identified in each relevant area of the licensee's operations, including all of the following:

(1) Employee training and management.

(2) Information systems, including network and software design; and information classification, governance, processing, storage, transmission, and disposal.

(3) Detection, prevention, and response to an attack, intrusion, or other system failure.

e. Implements information safeguards to manage threats identified in the licensee's ongoing risk assessments and, at least annually, assesses the effectiveness of the information safeguards' key controls, systems, and procedures.

4. Based on the risk assessment conducted pursuant to subsection 3, a licensee shall do all of the following:

a. Develop, implement, and maintain an information security program as described in subsections 1 and 2.

b. Determine which of the following security measures are appropriate and implement each appropriate security measure:

(1) 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.

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable the licensee to achieve its business purposes in accordance with the data, personnel, devices, systems, and facilities relative importance to the licensee's business objectives and risk strategy.

(3) Restrict access of nonpublic information stored in or at physical locations to authorized individuals only.

(4) Protect by encryption or other appropriate means, all nonpublic information while the nonpublic information is transmitted over an external network, and all nonpublic information that is stored on a laptop computer, a portable computing or storage device, or portable computing or storage media.

(5) Adopt secure development practices for in-house developed applications utilized by the licensee, and procedures for evaluating, assessing, and testing the security of externally developed applications utilized by the licensee.

(6) Modify information systems in accordance with the licensee's information security program.

(7) Utilize effective controls, which may include multi-factor authentication procedures for authorized individuals accessing nonpublic information.

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

(9) 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 the normal business operations and obligations of the licensee.

(10) Implement measures to protect against the destruction, loss, or damage of nonpublic information due to environmental hazards, natural disasters, catastrophes, or technological failures.

(11) Develop, implement, and maintain procedures for the secure disposal of nonpublic information that is contained in any format.

c. Include cybersecurity risks in the licensee's enterprise-wide risk management process.

d. Maintain knowledge and understanding of emerging threats or vulnerabilities and utilize reasonable security measures, relative to the character of the sharing and the type of information being shared, when sharing information.

e. Provide the licensee's personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee's risk assessment.

5. *a.* If a licensee has a board of directors, the board or an appropriate committee of the board shall at a minimum require the licensee's executive management or the executive management's delegates to:

(1) Develop, implement, and maintain the licensee's information security program.

(2) Provide a written report to the board, at least annually, that documents all of the following:

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

(b) Material matters related to the licensee's information security program including issues such as risk assessment; risk management and control decisions; third-party service provider arrangements; results of testing, cybersecurity events, or violations; management's response to cybersecurity events or violations; and recommendations for changes in the licensee's information security program.

b. If a licensee's executive management delegates any of its responsibilities under this section the executive management shall oversee the delegate's development, implementation, and maintenance of the licensee's information security program, and shall require the delegate to submit an annual written report to executive management that contains the information required under paragraph "*a*", subparagraph (2). If the licensee has a board of directors, the executive management shall provide a copy of the report to the board.

6. A licensee shall monitor, evaluate, and adjust the licensee's information security program consistent with relevant changes in technology, the sensitivity of the licensee's

nonpublic information, changes to the licensee's information systems, internal or external threats to the licensee's nonpublic information, and the licensee's changing business arrangements, including but not limited to mergers and acquisitions, alliances and joint ventures, and outsourcing arrangements.

7. As part of a licensee's information security program, a 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 nonpublic information in the licensee's possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's operations. The written incident response plan must address all of the following:

a. The licensee's internal process for responding to a cybersecurity event.

b. The goals of the licensee's incident response plan.

c. The assignment of clear roles, responsibilities, and levels of decision-making authority for the licensee's personnel that participate in the incident response plan.

d. External communications, internal communications, and information sharing related to a cybersecurity event.

e. The identification of remediation requirements for weaknesses identified in information systems and associated controls.

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

g. The evaluation and revision of the incident response plan, as appropriate, following a cybersecurity event.

8. An insurer domiciled in this state shall annually submit to the commissioner on or before April 15 a written certification that the insurer is in compliance with this section. Each insurer shall maintain all records, schedules, documentation, and data supporting the insurer's certification for five years. To the extent an insurer has identified an area, system, or process that requires material improvement, updating, or redesign, the insurer shall document the process used to identify the area, system, or process, and the remediation that has been implemented, or will be implemented, to address the area, system, or process. All records, schedules, documentation, and data described in this subsection shall be made available for inspection by the commissioner, or the commissioner's representative, upon request of the commissioner.

9. Licensees shall comply with this section no later than January 1, 2023.

2021 Acts, ch 79, §4, 17
Referred to in §507F.3