304.3-756 Written information security program -- Requirements -- Assessments -- Written incident response plan -- Annual certification to commissioner.

(1) As used in this section:

(a) "Authorized individual" means an individual:

1. Known to, and screened by, the licensee; and

2. Determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information systems;

(b) "Multi-factor authentication" means authentication through verification of at least two (2) of the following methods of authentication factors:

1. Knowledge factors, such as a password;

2. Possession factors, such as a token or text message on a mobile phone; or

3. Inherence factors, such as a biometric characteristic; and

(c) "Risk assessment" means the risk assessment that each licensee is required to conduct under subsection (3) of this section.

(2) (a) Each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(b) The information security program required under this subsection shall be:

1. Commensurate with the:

a. Size and complexity of the licensee;

b. Nature and scope of the licensee's activities, including its use of third-party service providers; and

c. Sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control; and

2. Designed to:

a. Protect the security and confidentiality of nonpublic information and the security of the information system;

b. Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;

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

d. Define, and periodically reevaluate:

i. A schedule for retention of nonpublic information; and

ii. A mechanism for the destruction of nonpublic information when no longer needed, which shall comply with KRS 365.725.

(3) Each licensee shall:

(a) Designate one (1) or more employees, an affiliate, or an outside vendor

designated to act on behalf of the licensee who is responsible for the information security program;

(b) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers;

(c) Assess the likelihood and potential damage of the threats identified under paragraph (b) of this subsection, taking into consideration the sensitivity of the nonpublic information;

(d) Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage the threats identified under paragraph (b) of this subsection, including consideration of threats in each relevant area of the licensee's operations, including:

1. Employee training and management;
2. Information systems, including network and software design, information classification, governance, processing, storage, transmission, and disposal; and
3. Detection, prevention, and response to attacks, intrusions, or other system failures;

(e) Implement information safeguards to manage the threats identified in the licensee's ongoing assessment; and

(f) No less than annually, assess the effectiveness of the key controls, systems, and procedures of the safeguards implemented under paragraph (e) of this subsection.

(4) Based on its risk assessment, each licensee shall:

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

1. Size and complexity of the licensee; and
2. Nature and scope of the licensee's activities, including its use of third-party service providers;

(b) Implement the following security measures, as appropriate:

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 organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;
3. Restrict physical access to nonpublic information to authorized individuals only;
4. Protect, by encryption or other appropriate means, all nonpublic information:

a. While being transmitted over an external network; and

b. Stored on a laptop computer or other portable computing or storage device or media;

5. Adopt:

a. Secure development practices for in-house developed applications utilized by the licensee; and

b. Procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee;

6. Modify the information system in accordance with the licensee's information security program;

7. Utilize effective controls, which may include multi-factor authentication procedures for any individual 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:

a. Detect and respond to cybersecurity events; and

b. Reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

10. 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

11. Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format;

(c) Include cybersecurity risks in the licensee's enterprise risk management process;

(d) Stay informed regarding emerging threats or vulnerabilities;

(e) Utilize reasonable security measures when sharing information commensurate with the character of the sharing and the type of information shared; and

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

(5) (a) A licensee's executive management or its delegates shall, at a minimum:

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

2. If the licensee has a board of directors or other appropriate committee, report at least annually, in writing, to the board or committee the following information:

a. The overall status of the information security program and the licensee's compliance with KRS 304.3-750 to 304.3-768; and

b. Material matters related to the information security program, addressing issues including risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and

management's response to the events or violations, and recommendations for changes in the information security program.

(b) If a licensee's executive management delegates any of its responsibilities under this subsection, executive management shall:

1. Oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegate or delegates; and

2. Receive a report from the delegate or delegates that complies with the requirements of paragraph (a)2. of this subsection.

(6) Each licensee that uses a third-party service provider shall:

(a) Exercise due diligence in selecting the third-party service provider; and

(b) Require the 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.

(7) Each licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with:

(a) Any relevant changes in technology;

(b) The sensitivity of its nonpublic information;

(c) Internal or external threats to information; and

(d) The licensee's own changing business arrangements, including mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(8) (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:

1. The confidentiality, integrity, or availability of nonpublic information in its possession;

2. The licensee's information systems; or

3. The continuing functionality of any aspect of the licensee's business or operations.

(b) The incident response plan established under this subsection shall address the following:

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.

(9) (a) Each insurer domiciled in this state shall:

1. By February 15 of each year, submit to the commissioner a written statement certifying that the insurer is in compliance with this section; and

2. Maintain, for examination by the department, all records, schedules, and data supporting the certification submitted under subparagraph 1. of this paragraph for a period of five (5) years.

(b) 1. 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 remedial efforts planned and underway to address the areas, systems, or processes identified.

2. The documentation required under this paragraph shall be available for inspection by the commissioner for a period of five (5) years.

(10) (a) An employee, agent, representative, or designee of a licensee, who is also a licensee, shall be exempt from the requirements of this section and shall not be required to develop its own information security program to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(b) In the event that a licensee ceases to qualify for an exception under paragraph (a) of this subsection, the licensee shall have one hundred eighty (180) days to comply with this section.

Effective: January 1, 2023

History: Created 2022 Ky. Acts ch. 149, sec. 4, effective January 1, 2023.