# Tenn. Code Ann. § 56-2-1004





## 56-2-1004. Information security program.

By July 1, 2022, unless provided otherwise in this section:

**(1)** Commensurate with the size and complexity of the licensee and the nature and scope of its activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by or in the possession, custody, or control of the licensee, 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 the nonpublic information and the licensee's information system;

**(2)** A licensee's information security program must be designed to:

**(A)** Protect the security and confidentiality of nonpublic information and the security of the information system;

**(B)** Protect against 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 a consumer as a result of unauthorized access or use; and

**(D)** Define and periodically reevaluate a schedule for retaining nonpublic information and a mechanism for the destruction of nonpublic information when the information is no longer needed;

**(3)** A licensee shall conduct a risk assessment as follows:

**(A)** Designate one (1) or more employees, an affiliate, or an outside vendor acting on behalf of the licensee who is responsible for the licensee's 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 threats to the security of information systems and nonpublic information accessible to or held by third-party service providers;

**(C)** Assess the likelihood and potential damage of reasonably foreseeable internal or external threats, taking into consideration the sensitivity of the nonpublic information involved;

**(D)** Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage threats throughout the licensee's operations, including in:

**(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)** Detection, prevention, and response to attacks, intrusions, or other information systems failures; and

**(E)** Implement information safeguards to manage the threats identified in the licensee's risk assessment and, no less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures;

**(4)** Based on a licensee's risk assessment, the licensee shall:

**(A)** Design an information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee and the nature and scope of its activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by or in the possession, custody, or control of the licensee;

**(B)** Determine which of the following security measures are appropriate for the licensee and implement those security measures:

**(i)** Place access controls on information systems, including controls to authenticate and restrict access 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 licensee to achieve the licensee's business objectives in accordance with the relative importance of the data, personnel, devices, systems, and facilities to the licensee's business objectives and risk strategy;

**(iii)** Restrict physical access to nonpublic information to authorized individuals;

**(iv)** Protect by encryption or other appropriate means nonpublic information being transmitted over an external network and nonpublic information stored on a laptop computer or other portable computing or storage device or media;

**(v)** Adopt secure development practices for internally developed applications utilized by the licensee and procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee;

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

**(vii)** Utilize effective controls that may include multi-factor authentication procedures for authorized individuals 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 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, technological failures, or other catastrophic events; and

**(xi)** 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)** Remain informed regarding emerging threats or vulnerabilities to the licensee and utilize reasonable security measures when sharing information, relative to the nature of the sharing and the type of information being shared; or

**(E)** Provide personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment;

**(5)** If the licensee has a board of directors, then the board or an appropriate committee of the board shall, at a minimum:

**(A)** Require the licensee's executive management or delegates to develop, implement, and maintain the licensee's information security program;

**(B)** Require the licensee's executive management or delegates to report in writing, at least annually:

**(i)** The status of the licensee's information security program and compliance with this part; and

**(ii)** Material matters related to the licensee's information security program, including risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and the licensee's responses thereto, and recommendations for changes to the information security program; and

**(C)** If the licensee's executive management delegates any of the executive management's responsibilities under this section, then the executive management must oversee the development, implementation, and maintenance of the licensee's information security program prepared by the delegates and must either prepare the report or receive a copy of the report prepared by the delegates pursuant to subdivision (5)(B);

**(6)** A licensee shall exercise due diligence in selecting a third-party service provider and, by July 1, 2023, require that each third-party service provider implement appropriate

administrative, technical, and physical measures to protect and secure the information systems and nonpublic information accessible to, or held by, the third-party service provider;

**(7)** The licensee shall monitor, evaluate, and adjust, as appropriate, its information security program, consistent with relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to its information, and its changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems;

**(8)**

**(A)** As part of a licensee's information security program, a licensee must 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 the licensee's nonpublic information or information systems or the continuing functionality of the licensee's operations;

**(B)** The incident response plan must address:

**(i)** The licensee's internal process for responding to a cybersecurity event;

**(ii)** The goals of the licensee's incident response plan;

**(iii)** The definition of roles, responsibilities, and levels of decision-making authority relating to a cybersecurity event;

**(iv)** External and internal communications and information sharing;

**(v)** The requirements for remediating identified weaknesses in information systems and associated controls;

**(vi)** Documentation and reporting regarding cybersecurity events and related incident response activities; and

**(vii)** The evaluation and revision, as necessary, of the incident response plan following a cybersecurity event; and

**(9)**

**(A)** Each insurer domiciled in this state shall submit to the commissioner by April 15 of each year written certification that the insurer is in compliance with this section. Each insurer shall maintain for examination by the department all records, schedules, and data supporting the certification for a period of five (5) years from the date of the corresponding certification.

**(B)** If an insurer identifies areas, systems, or processes requiring material improvement, updating, or redesign, then the insurer must document planned and ongoing remedial efforts to address those areas, systems, or processes, and the documentation must be made available for inspection by the commissioner upon request.

## History

Acts 2021, ch. 345, § 1.

End of Document