46A.03 ELEMENTS.

Subdivision 1. **Generally.** In order to develop, implement, and maintain an information security program, a financial institution must comply with this section.

Subd. 2. **Qualified individual.** (a) A financial institution must designate a qualified individual responsible for overseeing, implementing, and enforcing the financial institution's information security program. The qualified individual may be employed by the financial institution, an affiliate, or a service provider.

(b) If a financial institution designates an individual employed by an affiliate or service provider as the financial institution's qualified individual, the financial institution must:

(1) retain responsibility for complying with this chapter;

(2) designate a senior member of the financial institution's personnel to be responsible for directing and overseeing the qualified individual's activities; and

(3) require the service provider or affiliate to maintain an information security program that protects the financial institution in a manner that complies with the requirements of this chapter.

Subd. 3. **Security risk assessment.** (a) A financial institution must base the financial institution's information security program on a risk assessment that:

(1) identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that might result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of customer information; and

(2) assesses the sufficiency of any safeguards in place to control the risks identified under clause (1).

(b) The risk assessment must be made in writing and must include:

(1) criteria to evaluate and categorize identified security risks or threats the financial institution faces;

(2) criteria to assess the confidentiality, integrity, and availability of the financial institution's information systems and customer information, including the adequacy of existing controls in the context of the identified risks or threats the financial institution faces; and

(3) requirements describing how:

(i) identified risks are mitigated or accepted based on the risk assessment; and

(ii) the information security program addresses the risks.

(c) A financial institution must periodically perform additional risk assessments that:

(1) reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that might result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of customer information; and

(2) reassess the sufficiency of any safeguards in place to control the risks identified under clause (1).

Subd. 4. **Risk control.** A financial institution must design and implement safeguards to control the risks the financial institution identifies through the risk assessment under subdivision 3, including by:

(1) implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:

(i) authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

(ii) limit an authorized user's access to only customer information that the authorized user needs to perform the authorized user's duties and functions or, in the case of a customer, to limit access to the customer's own information;

(2) identifying and managing the data, personnel, devices, systems, and facilities that enable the financial institution to achieve business purposes in accordance with the business purpose's relative importance to business objectives and the financial institution's risk strategy;

(3) protecting by encryption all customer information held or transmitted by the financial institution both in transit over external networks and at rest. To the extent a financial institution determines that encryption of customer information either in transit over external networks or at rest is infeasible, the financial institution may secure the customer information using effective alternative compensating controls that have been reviewed and approved by the financial institution's qualified individual;

(4) adopting: (i) secure development practices for in-house developed applications utilized by the financial institution to transmit, access, or store customer information; and (ii) procedures to evaluate, assess, or test the security of externally developed applications the financial institution uses to transmit, access, or store customer information;

(5) implementing multifactor authentication for any individual that accesses any information system, unless the financial institution's qualified individual has approved in writing the use of a reasonably equivalent or more secure access control;

(6) developing, implementing, and maintaining procedures to securely dispose of customer information in any format no later than two years after the last date the information is used in connection with providing a product or service to the customer to whom the information relates, unless: (i) the information is necessary for business operations or for other legitimate business purposes; (ii) the information is otherwise required to be retained by law or regulation; or (iii) targeted disposal of the information is not reasonably feasible due to the manner in which the information is maintained;

(7) periodically reviewing the financial institution's data retention policy to minimize the unnecessary retention of data;

(8) adopting procedures for change management; and

(9) implementing policies, procedures, and controls designed to: (i) monitor and log the activity of authorized users; and (ii) detect unauthorized access to, use of, or tampering with customer information by authorized users.

Subd. 5. **Testing and monitoring.** (a) A financial institution must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including the controls, systems, and procedures that detect actual and attempted attacks on, or intrusions into, information systems.

(b) For information systems, monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems

to detect on an ongoing basis any changes in information systems that may create vulnerabilities, a financial institution must conduct:

(1) annual penetration testing of the financial institution's information systems, based on relevant identified risks in accordance with the risk assessment; and

(2) vulnerability assessments, including systemic scans or information systems reviews that are reasonably designed to identify publicly known security vulnerabilities in the financial institution's information systems based on the risk assessment, at least every six months, whenever a material change to the financial institution's operations or business arrangements occurs, and whenever the financial institution knows or has reason to know circumstances exist that may have a material impact on the financial institution's information security program.

Subd. 6. **Internal policies and procedures.** A financial institution must implement policies and procedures to ensure that the financial institution's personnel are able to enact the financial institution's information security program by:

(1) providing the financial institution's personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) utilizing qualified information security personnel employed by the financial institution, an affiliate, or a service provider sufficient to manage the financial institution's information security risks and to perform or oversee the information security program;

(3) providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

Subd. 7. **Provider oversight.** A financial institution must oversee service providers by:

(1) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

(2) requiring by contract the financial institution's service providers to implement and maintain appropriate safeguards; and

(3) periodically assessing the financial institution's service providers based on the risk the service providers present and the continued adequacy of the service providers' safeguards.

Subd. 8. **Information security program; evaluation; adjustment.** A financial institution must evaluate and adjust the financial institution's information security program to reflect: (1) the results of the testing and monitoring required under subdivision 5; (2) any material changes to the financial institution's operations or business arrangements; (3) the results of risk assessments performed under subdivision 3, paragraph (c); or (4) any other circumstances that the financial institution knows or has reason to know may have a material impact on the financial institution's information security program.

Subd. 9. **Incident response plan.** A financial institution must establish a written incident response plan designed to promptly respond to and recover from any security event materially affecting the confidentiality, integrity, or availability of customer information the financial institution controls. An incident response plan must address:

(1) the goals of the incident response plan;

(2) the internal processes to respond to a security event;

(3) clear roles, responsibilities, and levels of decision-making authority;

(4) external and internal communications and information sharing;

(5) requirements to remediate any identified weaknesses in information systems and associated controls;

(6) documentation and reporting regarding security events and related incident response activities; and

(7) evaluation and revision of the incident response plan as necessary after a security event.

Subd. 10. **Annual report.** (a) A financial institution must require the financial institution's qualified individual to report at least annually in writing to the financial institution's board of directors or equivalent governing body. If a board of directors or equivalent governing body does not exist, the report under this subdivision must be timely presented to a senior officer responsible for the financial institution's information security program.

(b) The report made under this subdivision must include the following information:

(1) the overall status of the financial institution's information security program, including compliance with this chapter and associated administrative rules; and

(2) material matters related to the financial institution's information security program, including but not limited to addressing issues pertaining to: (i) the risk assessment; (ii) risk management and control decisions; (iii) service provider arrangements; (iv) testing results; (v) security events or violations and management's responses to the security event or violation; and (vi) recommendations for changes in the information security program.

Subd. 11. **Business continuity; disaster recovery.** A financial institution must establish a written plan addressing business continuity and disaster recovery.

History: *2024 c 114 art 2 s 3*