60A.981 INFORMATION SECURITY PROGRAM.

Subdivision 1. **General requirements.** Each licensee shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of customer information. The administrative, technical, and physical safeguards included in the information security program must be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Subd. 2. **Objectives.** A licensee's information security program must be designed to:

(1) ensure the security and confidentiality of customer information;

(2) protect against any anticipated threats or hazards to the security or integrity of the information; and

(3) protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Subd. 3. **Examples of methods of development and implementation.** The following actions and procedures are examples of methods of implementation of the requirements of subdivisions 1 and 2. These examples are nonexclusive illustrations of actions and procedures that licensees may follow to implement subdivisions 1 and 2:

(1) the licensee:

(i) identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

(ii) assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

(iii) assesses the sufficiency of policies, procedures, customer information systems, and other safeguards in place to control risks;

(2) the licensee:

(i) designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;

(ii) trains staff, as appropriate, to implement the licensee's information security program; and

(iii) regularly tests or otherwise regularly monitors the key controls, systems, and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment;

(3) the licensee:

(i) exercises appropriate due diligence in selecting its service providers; and

(ii) requires its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations; and

(4) the licensee monitors, evaluates, and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer 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 customer information systems.

History: *2005 c 132 s 7*