

## CHAPTER 45-14-02 INFORMATION SECURITY PROGRAM

### Section

45-14-02-01	Definitions
45-14-02-02	Information Security Program
45-14-02-03	Developing and Implementing an Information Security Program

#### **45-14-02-01. Definitions.**

As used in this chapter:

1. "Customer" means "customer" as defined in section 45-14-01-04.
2. "Customer information" means "nonpublic personal financial information", as defined in section 45-14-01-04, about a customer, whether in paper, electronic, or other form that is maintained by or on behalf of the licensee.
3. "Customer information system" means the methods used to access, collect, store, use, transmit, protect, or dispose of customer information.
4. "Licensee" means "licensee" as defined in section 45-14-01-04.
5. "Service provider" means a person that provides services to the licensee and maintains, possesses, or otherwise is permitted access to customer information.

**History:** Effective October 1, 2004.

**General Authority:** NDCC 28-32-02

**Law Implemented:** NDCC 26.1-02-27

#### **45-14-02-02. Information security program.**

Each licensee shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of customer information that is appropriate to the size and complexity of the licensee and the nature and scope of its activities. Each information security program shall be designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to, or use of, customer information that could result in substantial harm or inconvenience to any customer.

**History:** Effective October 1, 2004.

**General Authority:** NDCC 28-32-02

**Law Implemented:** NDCC 26.1-02-27

#### **45-14-02-03. Developing and implementing an information security program.**

The actions and procedures described in this section are examples of methods of implementation of this chapter. These examples are nonexclusive illustrations of practices and procedures that a licensee may follow to implement this chapter.

1. Each licensee identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. Each licensee assesses the likelihood and potential damage of the risks presented by the threats it has identified, taking into consideration the sensitivity of customer information. Each licensee assesses the sufficiency of the policies and procedures it has in place to control the risks it has identified.

2. Each information security program is designed to control the identified risks, commensurate with the sensitivity of the information and the complexity and scope of the licensee's activities. Each licensee trains staff, as appropriate, to implement the licensee's information security program and regularly tests or otherwise monitors the key controls, systems, and procedures of its information security program.
3. Each licensee exercises due diligence in selecting service providers and obtains satisfactory assurances from the service provider that it will appropriately safeguard the information to meet the objectives of section 45-14-02-02.
4. Each licensee monitors, evaluates, and adjusts, as appropriate, its information security program to reflect 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 its customer information systems.

**History:** Effective October 1, 2004.

**General Authority:** NDCC 28-32-02

**Law Implemented:** NDCC 26.1-02-27