

## **Information Security Program Charter - DRAFT COPY**

Information is an essential State of North Dakota asset and is vitally important to State of North Dakota's business operations and delivery of services. The State of North Dakota must ensure that its information assets are protected in a manner that is cost-effective and that reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

The State of North Dakota's Information Security Program will adopt a risk management approach to Information Security. The risk management approach requires the identification, assessment, and appropriate mitigation of vulnerabilities and threats that can adversely impact State of North Dakota's information assets.

This Information Security Program Charter serves as the "capstone" document for the State of North Dakota's Information Security Program.

### **I. Scope**

This Information Security Program Charter and associated policies, standards, guidelines, and procedures apply to all employees, contractors, part-time and temporary workers, and those employed by others to perform work on State of North Dakota premises or who have been granted access to State of North Dakota information or systems.

### **II. Information Security Program Mission Statement**

The State of North Dakota Information Security Program will use a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures that address security objectives in tandem with business and operational considerations.

The Information Security Program will develop policies to define protection and management objectives for information assets. The Information Security Program will also define acceptable use of State of North Dakota information assets.

The Information Security Program will attempt to reduce vulnerabilities by developing policies to monitor, identify, assess, prioritize, and manage vulnerabilities and threats. The management activities will support organizational objectives for mitigating, responding to and recovering from identified vulnerabilities and threats.

The Information Security Program will ensure that the Information Security Program Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood by establishing a Security Awareness Program to educate and train the individuals, groups, and agencies covered by the scope of this Charter.

### **III. Ownership and Responsibilities**

The Chief Information Officer (CIO) approves the State of North Dakota Information Security Program Charter. The Information Security Program Charter assigns executive ownership of and accountability for the State of North Dakota Information Security Program to the Chief Information Officer (CIO). The CIO must approve Information Security policies.

The CIO will appoint a Chief Information Security Officer (CISO) to implement and manage the Information Security Program across the State of North Dakota. The CISO is responsible for the development of State of North Dakota Information Security policies, standards and guidelines. The CISO must approve Information Security standards and guidelines, and ensure their consistency with approved Information Security policies. The CISO also will establish an Information Security Awareness Program to ensure that the Information Security Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood across the State of North Dakota.

The Chief Information Security Officer (CISO) will establish a list of Agency Security Officers. The Lead IT Coordinator of each agency will be designated the Agency Security Officer unless the agency designates someone else. The role of the Agency Security Officer includes submitting security requests, reviewing access logs, reviewing authorization reports, and being the main point of contact between ITD and the agency regarding security issues.

ITD is accountable for the execution of the State of North Dakota Information Security Program and ensuring that the Information Security Program Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood within State of North Dakota agencies. State agencies are responsible for defining, approving and implementing Information Security procedures in their agencies and ensuring their consistency with approved Information Security policies and standards.

All individuals, groups, or organizations identified in the scope of this Charter are responsible for familiarizing themselves with the State of North Dakota Information Security Program Charter and complying with its associated policies.

#### **IV. Enforcement and Exception Handling**

Failure to comply with State of North Dakota Information Security policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to State of North Dakota Information Security policies, standards, and guidelines should be made on the Request for Exceptions to Information Technology Standards & Policy form (SFN 51687) and submitted to the IT Planning Division of the Information Technology Department. Exceptions shall be permitted only on receipt of written approval from the Information Technology Department.

#### **V. Review and Revision**

The State of North Dakota Information Security policies, standards, and guidelines shall be reviewed under the supervision of the CISO, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness.

Approved: \_\_\_\_\_

Signature  
Curt Wolfe  
Chief Information Officer