State of Illinois
Department of Innovation & Technology
Enterprise Information Security Policy
Program Management Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) Program Management Policy coordinates activities to manage risk to an acceptable level and to provide protection of State of Illinois information assets utilizing Defense in Depth. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to protect State of Illinois information and Information Systems, to reduce cyber risk through sound risk management practices, and to provide best-in-class enterprise information security program capabilities to Illinois agencies, boards, and commissions.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to “Agency” below shall include both DoIT and Client Agencies.

4.1 Information Security Program Plan

4.1.1 Agency shall develop and disseminate an information security program plan that:

(1) provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

(2) includes the identification and assignment of roles, responsibilities, management commitment, coordination, and compliance;

(3) reflects coordination and responsibility for the different aspects of information security (i.e., technical, physical, personnel, and cyber-physical); and

(4) is approved by senior officials with responsibility and accountability for the reduction of risk to operations and mission objectives.

4.1.2 Agency shall review the security program plan based on a defined frequency.

4.1.3 Agency shall update the plan to address changes and problems identified during plan implementation or security control assessments.

4.1.4 Agency shall protect the information security program plan from unauthorized disclosure and modification.

4.2 Senior Information Security Officer

4.2.1 Agency shall appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an information security program.

4.3 Information Security Resources

4.3.1 Agency shall ensure that appropriate information security resources are allocated to implement the information security program.

4.4 Plan of Action and Milestones Process

4.4.1 Agency shall implement a process for ensuring that a Plan of Action and Milestones (POAM) or a Corrective Action Plan (CAP) is developed and maintained for the security program and associated Information Systems.

(1) Agency shall document the remedial information security actions to adequately respond to risk to operations and assets, individuals, and other organizations.

4.4.2 Agency shall review POAMs and CAPs for consistency with the risk management strategy and priorities for risk response.

4.5 Information System Inventory

4.5.1 Agency shall develop and maintain an inventory of Information Systems.

4.6 Information Security Measures of Performance

4.6.1 Agency shall develop, monitor, and report on the results of information security measures of performance.

4.7 Enterprise Architecture

4.7.1 Agency shall develop enterprise architecture with consideration for information security and the resulting risk to operations, assets, individuals, and other organizations.

4.8 Critical Infrastructure Plan

4.8.1 Agency shall address information security issues in the development, documentation, and updating of a critical infrastructure and key resource continuity plan.

4.9 Risk Management Strategy

4.9.1 Agency shall develop a comprehensive strategy to manage risk.

(1) Agency shall implement the risk management strategy.

(2) Agency shall review and update the risk management strategy based on a defined frequency or as necessary to address risk.

4.10 Security Authorization Process

4.10.1 Agency shall manage (i.e., document, track, and report) the level of security on Information Systems and the environments in which those systems operate through security authorization processes.

(1) Agency shall designate individuals to fulfill specific roles and responsibilities within the risk management process.

(2) Agency shall fully integrate the security authorization processes into its management program.

4.11 Mission/Business Process Definition

4.11.1 Agency shall define mission/business processes with consideration for information security and the resulting risk to operations, assets, individuals, and other organizations.

4.11.2 Agency shall determine information protection needs arising from the defined mission/business processes and shall revise the processes as necessary, until achievable protection needs are obtained.

4.12 Insider Threat Program

4.12.1 Agency shall implement an insider threat program that includes a cross-discipline, insider threat incident handling team.

4.13 Information Security Workforce

4.13.1 Agency shall establish an information security workforce development and improvement program.

4.14 Testing, Training, and Monitoring

4.14.1 Agency shall implement a process for ensuring that Agency plans for conducting security testing, training, and monitoring activities associated with Information Systems are developed and maintained, and that they continue to be executed in a timely manner.

4.14.2 Agency shall review testing, training, and monitoring plans for consistency with the Agency's risk management strategy and priorities for risk response actions.

4.15 Contacts with Security Groups and Associations

4.15.1 Agency shall establish and institutionalize contact with selected groups and associations within the security community to facilitate ongoing security education and training for personnel.

4.15.2 Agency shall remain current with recommended security practices, techniques, and technologies.

4.15.3 Agency shall share current security-related information including threats, vulnerabilities, and incidents.

4.16 Threat Awareness Programs

4.16.1 Agency shall implement a threat awareness program that includes information-sharing capabilities.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate responsibility to specific personnel. To the extent necessary, each Client Agency and/or DoIT Division must establish procedures in order to achieve Policy compliance. It is the responsibility of all Employees to understand and adhere to this Policy.

Failure to comply with this Policy may result in the Chief Information Security Officer temporarily discontinuing or suspending the operation of the Information System, solution, and/or resource until such compliance is established as deemed solely by the Chief Information Security Officer. Failure to comply with this Policy could also result in the loss of access to State of Illinois Information Technology (IT) Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.