State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
System and Services Acquisition

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) will protect the integrity of systems and information through the development, implementation, documentation, and maintenance of the below system and services acquisition requirements. This Policy defines the criteria and methods for managing risks associated with third-party products and service providers. 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 ensure consistent application of security controls across all State of Illinois systems during the procurement process.

3. SCOPE

This Policy applies to Users 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 Allocation of Resources

4.1.1 Agency shall determine information security requirements for the Information System or Information System service in mission/business process planning.

4.1.2 Agency shall determine, document, and allocate the resources required to protect the Information System or Information System service as part of its capital planning and investment control process.

4.1.3 Agency shall establish a discrete line item for information security in programming and budgeting documentation.

4.2 System Development Lifecycle

4.2.1 Agency shall manage the Information System using the DoIT-defined system development life cycle methodology that incorporates information security considerations.

4.2.2 Agency shall define and document information security roles and responsibilities throughout the system development life cycle.

4.2.3 Agency shall identify individuals having information security roles and responsibilities.

4.2.4 Agency shall integrate the information security risk management process into system development life cycle activities.

4.3 Acquisition Process

4.3.1 The following requirements, descriptions, and criteria, explicitly or by reference, will be included in the acquisition contract for the Information System, system component, or Information System service in accordance with applicable laws, executive orders, directives, policies, regulations, standards, guidelines, and as applicable to the Agency's mission/business needs:

- security functional requirements;
- security strength requirements;
- security assurance requirements;
- security-related documentation requirements;
- requirements for protecting security-related documentation;
- description of the Information System development environment and environment in which the system is intended to operate; and
- acceptance criteria.

4.4 Information System Documentation

4.4.1 Agency shall obtain administrator documentation for the Information System, system component, or Information System service that describes:

- secure configuration, installation, and operation of the system, component, or service;
- effective use and maintenance of security functions/mechanisms; and
- known vulnerabilities regarding configuration and use of administrative functions.

4.4.2 Agency shall obtain user documentation for the Information System, system component, or Information System service that describes:

- User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
- methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
- User responsibilities in maintaining the security of the system, component, or service.

4.4.3 Agency shall document each attempt to obtain Information System, component, or Information System service documentation, when unavailable.

4.4.4 Agency shall protect documentation as required, in accordance with Least Privilege risk management strategy.

4.4.5 Agency shall distribute documentation to appropriate personnel.

4.5 Security Engineering Principles

4.5.1 DoIT shall apply Information System security engineering principles in the specification, design, development, implementation, and modification of the Information System.

4.6 External Information System Services

4.6.1 Agency shall require that providers of external Information System services comply with DoIT information security requirements and employ security controls in accordance with applicable laws, executive orders, directives, policies, regulations, standards, and guidance.

4.6.2 Agency shall define and document oversight, User roles, and responsibilities.

4.6.3 Agency shall employ DoIT processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis.

4.7 Developer Configuration Management

4.7.1 Agency shall require the developer of the Information System, system component, or Information System service to:

- perform configuration management during system, component, or service for design, development, implementation, and operation;
- document, manage, and control the integrity of changes to configuration items under configuration management;
- implement only approved changes to the system, component, or service;
- document approved changes to the system, component, or service and the potential security impacts of such changes; and
- track security flaws and flaw resolution within the system, component, or service and report findings to appropriate personnel.

4.8 Developer Security Testing and Evaluation

4.8.1 Agency shall require the developer of the Information System, system component, or Information System service to:

- create and implement a security assessment plan;
- perform testing/evaluation per business requirements;
- produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
- implement a verifiable flaw remediation process; and
- correct flaws identified during security testing/evaluation.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security establishes supplemental policies, standards, procedures, and guidelines and designates 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 Users 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.