State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Risk Assessment

1. **Overview**

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for securing State of Illinois information technology (IT) assets from unauthorized access, modification, disclosure, and destruction. This Risk Assessment Policy addresses the establishment of policies and procedures for the effective implementation of selected security controls and control enhancements in the Risk Management Program. 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 that State of Illinois Information Systems are categorized and vulnerabilities are identified in order to allow management to make informed decisions.

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.

DoIT shall conduct all risk assessments.

4.1 Security Categorization

4.1.1 DoIT shall categorize information and the Information System in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
4.1.2 DoIT shall document the security categorization results (including supporting rationale) in the security plan for the Information System.
4.1.3 DoIT shall ensure that Agency senior management and appropriate designees review and approve the security categorization decision.

4.2 Risk Assessment

4.2.1 DoIT shall conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the Information System and the information it processes, stores, or transmits.
4.2.2 DoIT shall document risk assessment results and prepare a risk assessment report.
4.2.3 DoIT shall review risk assessment results.

4.2.4 DoIT shall disseminate risk assessment results to Agency senior management and appropriate designees.

4.2.5 DoIT shall update the risk assessment whenever there are significant changes to the Information System or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

4.3 Vulnerability Scanning

4.3.1 DoIT shall obtain authorization to scan for vulnerabilities in the Information Systems and hosted applications to identify threats.

4.3.2 DoIT shall employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

(1) enumerating platforms, software flaws, and improper configurations;
(2) formatting checklists and test procedures; and
(3) measuring vulnerability impact.

4.3.3 DoIT shall analyze vulnerability scan reports and results from security control assessments.

4.3.4 DoIT shall remediate legitimate vulnerabilities in accordance with an Agency assessment of risk.

4.3.5 DoIT shall share information obtained from the vulnerability scanning process and security control assessments with Agency senior management and appropriate designees to help eliminate similar vulnerabilities in other Information Systems (i.e., systemic weaknesses or deficiencies).

5. <u>POLICY COMPLIANCE</u>

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 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 IT Resources and/or discipline, up to and including discharge.

6. <u>RELATED POLICIES, STANDARDS, AND GUIDELINES</u>

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.