State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
System and Information Integrity

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for protecting the integrity of systems and information through the development, implementation, documentation, and maintenance of system and information integrity controls. 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 the integrity of State of Illinois data and Information Systems and to establish a consistent and enterprise-wide information security baseline.

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 Flaw Remediation

4.1.1 Agency shall identify, report, and correct Information System flaws.

4.1.2 Agency shall test software and firmware updates related to flaw remediation for effectiveness and potential side effects prior to implementation.

4.1.3 DoIT shall install applicable security-related software and firmware updates in compliance with standards established by the DoIT Division of Information Security.

4.1.4 DoIT shall incorporate flaw remediation into the Information System configuration processes.

4.2 Malicious Code Protection

4.2.1 DoIT shall employ malicious code protection mechanisms at Information System entry and exit points to detect and eradicate malicious code.

4.2.2 DoIT shall update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policies, standards, and/or procedures.

4.2.3 DoIT shall configure malicious code protection mechanisms to:

- perform periodic scans of the Information Systems;
- perform real-time scans of files from external sources at endpoints;
- block and quarantine malicious code;
- alert the DoIT Division of Information Security when suspected malicious code is detected;

- address the potential impact on the confidentiality, integrity, and availability of the impacted system and information; and
- address the receipt of false positives during malicious code detection and eradication.

4.3 Information System Monitoring

4.3.1 DoIT shall monitor Information Systems to detect:
- attacks and indicators of potential attacks in accordance with continuous monitoring policies, standards, and procedures; and
- unauthorized local, network, and remote connections.

4.3.2 DoIT shall identify unauthorized use of Information System(s) through system alerts and monitoring of system events/transactions.

4.3.3 DoIT shall deploy monitoring devices and/or capabilities strategically to collect essential information and at ad hoc locations to track specific types of transactions in support of attack detection and incident response.

4.3.4 DoIT shall protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

4.3.5 DoIT shall heighten the level of Information System monitoring activity whenever there is an indication of increased risk to Agency operations and assets, individuals, the State of Illinois, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

4.3.6 DoIT shall perform Information System monitoring activities in accordance with applicable laws, regulations, orders, directives, or policies.

4.3.7 Agency shall alert information security response personnel in line with established policies, standards, and plans when indications of compromise occur.

4.3.8 DoIT shall monitor inbound and outbound communications traffic on an ongoing basis to guard against unusual or unauthorized activities or conditions.

4.4 Security Alerts, Advisories, and Directives

4.4.1 Agency shall receive information security alerts, advisories, and directives on an ongoing basis from external organizations such as the Illinois Statewide Terrorism Intelligence Center, the United States Computer Emergency Readiness Team (US-CERT), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Department of Homeland Security (DHS).

4.4.2 Agency shall review the information security alerts or advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response.

4.4.3 Agency shall generate internal security alerts, advisories, and directives as deemed necessary.

4.4.4 Agency shall disseminate security alerts, advisories, and directives to personnel responsible for implementing, monitoring, and managing the Information System.

4.5 Spam Protection

4.5.1 DoIT shall employ spam protection mechanisms at Information System entry and exit points to detect and take action on unsolicited messages.

4.5.2 DoIT shall automatically update spam protection mechanisms when new releases are available.

4.6 Information Input Validation

4.6.1 Agency's Information Systems shall validate inputs to match specified definitions for format and content to ensure the confidentiality, integrity, and availability of the data.

4.7 Error Handling

4.7.1 Agency's Information Systems shall generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

4.7.2 Agency's Information Systems shall reveal error messages only to authorized personnel.

4.8 Information Handling and Retention

4.8.1 Agency's Information Systems shall handle and retain information within the system and output from the system in accordance with applicable laws, regulations, orders, directives, or policies.

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.