State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
System Maintenance

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for the establishment and implementation of appropriate system maintenance controls that safeguard the confidentiality, integrity, and availability of Information Systems. This Policy alleviates security risks by managing risks from information asset maintenance and repairs through the establishment of an effective system maintenance 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 protect State of Illinois Information Systems by establishing the minimum requirements for system maintenance.

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 Controlled Maintenance

4.1.1 Agency shall schedule, perform, document, and review records of maintenance and repairs on Information System components in accordance with manufacturer or vendor specifications and/or Agency requirements.

4.1.2 Agency shall approve and monitor all maintenance activities, whether performed on-site or remotely and whether the equipment is serviced on-site or removed to another location.

4.1.3 Agency shall require that defined personnel explicitly approve the removal of the Information System or system components from Agency facilities for off-site maintenance or repairs.

4.1.4 Agency shall sanitize equipment to remove all information from associated media prior to removal from Agency facilities for off-site maintenance or repairs.

4.1.5 DoIT shall test potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

4.1.6 Agency shall maintain system maintenance records.

4.2 Maintenance Tools

4.2.1 DoIT shall approve, control, and monitor Information System maintenance tools.

4.3 Non-Local Maintenance

4.3.1 Agency shall approve and monitor non-local maintenance and diagnostic activities.
4.3.2 DoIT shall approve the use of non-local maintenance and diagnostic tools.
4.3.3 DoIT shall employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.
4.3.4 DoIT shall maintain records for non-local maintenance and diagnostic activities.
4.3.5 DoIT shall terminate session and network connections when non-local maintenance is completed.

4.4 Maintenance Personnel

4.4.1 Agency shall establish a process for maintenance personnel authorization and shall maintain a list of authorized maintenance organizations or personnel.
4.4.2 Agency shall ensure that personnel performing maintenance on the Information System have required access authorizations and are supervised.

4.5 Timely Maintenance

4.5.1 Agency shall obtain maintenance support and/or spare parts for key components as defined in service agreements.

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.