1. OVERVIEW

The State of Illinois Department of Innovation and Technology (DoIT) is responsible for the establishment and implementation of media protection controls to protect electronic and physical media containing State information while at rest, stored, in transit, or actively being accessed. State Information Systems must be protected against improper or unauthorized access that could result in the compromise of confidentiality, integrity, or availability of State of Illinois information assets. 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 reduce the security risk to electronic or physical media containing State of Illinois information and to limit potential mishandling or loss while being stored, accessed, or transported to and from the Information Systems.

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" shall include both DoIT and Client Agencies.

4.1 Media Access

4.1.1 Agency shall restrict access to sensitive information residing on electronic and physical media to authorized individuals.

4.2 Media Storage

4.2.1 Agency shall:

- physically control and securely store all media in a secure area.
- encrypt digital media according to the classification of the data and secure non-digital media in secured environments.
- protect all Information System media until destroyed or sanitized using approved procedures.

4.3 Media Transport

4.3.1 Agency shall maintain accountability, protect Information System media during transport outside of controlled areas, and document associated activities. To protect the confidentiality and integrity of information stored on digital media and cryptographic mechanisms, Agency must implement FIPS 140-2 during transport outside of controlled areas.

4.4 Media Sanitization

4.4.1 Agency shall sanitize Information System media prior to disposal or release for reuse in accordance with applicable federal and state laws and regulations and Agency standards and policies. Agency shall use sanitation mechanisms that have the strength and integrity equivalent to the security category or classification of the information. Agency shall review, approve, track, document, and verify media sanitization and disposal actions.

4.5 Media Use

4.5.1 Agency shall restrict the use of personally owned media on Agency Information Systems or system components utilizing defined security safeguards.

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 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.