Enterprise Information Security Policy
Physical and Environmental Protection Policy

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for protecting information technology (IT) assets and the premises in which they reside. This Policy addresses the establishment and implementation for protecting IT assets from physical and environmental threats in order to reduce the risk of loss, theft, accidental damage, or unauthorized access to those IT 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 protect IT assets by limiting and controlling physical access and implementing controls to protect the physical environment in which State of Illinois IT assets are housed.

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 Physical Access Authorization

4.1.1 Agency shall develop, approve, and maintain an authorized access list of individuals with authorized access to the facility where the Information System resides.
4.1.2 Agency shall issue authorization credentials for access to the facility.
4.1.3 Agency shall review the access list detailing authorized facility access by individuals.
4.1.4 Agency shall remove individuals from the facility access list when access is no longer required.

4.2 Physical Access Control

4.2.1 Agency shall enforce physical access authorizations at defined entry/exit points to facilities where the Information Systems reside.
(1) Agency shall verify individual access authorization before granting access to the facility.
(2) Agency shall control ingress/egress to the facility.
4.2.2 Agency shall maintain physical access audit logs for defined entry/exit points.
4.2.3 Agency shall provide defined security safeguards to control access to areas within the facility officially designated as publicly accessible.
4.2.4 Agency shall monitor visitor activity.
4.2.5 Agency shall secure keys, combinations, and other physical access devices.
4.2.6 Agency shall inventory defined physical access devices on a defined frequency.
4.2.7 Agency shall change combinations and keys on a defined frequency and/or when keys are lost,

combinations are compromised, or individuals are transferred or terminated.

4.3 Access Control for Transmission Medium

4.3.1 Agency shall control physical access to defined Information System distribution and transmission lines within facilities using physical safeguards.

4.4 Access Control for Output Devices

4.4.1 Agency shall control physical access to Information System output devices to prevent unauthorized individuals from obtaining the output.

4.5 Monitoring Physical Access

4.5.1 Agency shall monitor physical access to the facility where information resides to detect and respond to physical security incidents.

4.5.2 Agency shall review physical access logs on a defined frequency and upon the occurrence and/or indication of adverse events.

4.5.3 Agency shall review and investigate physical security incidents through a formally developed response process.

4.6 Visitor Access Records

4.6.1 Agency shall maintain visitor access records to the facility where the Information System resides for a defined time period.

4.6.2 Agency shall review access records on a defined frequency.

4.7 Power Equipment and Cabling

4.7.1 Agency shall protect power equipment and power cabling for the Information System from damage and destruction.

4.8 Emergency Shutoff

4.8.2 Agency shall provide the capability of shutting off power to the Information System or individual system components in emergency situations.

4.8.3 Agency shall place emergency shutoff switches or devices to facilitate safe and easy access for personnel.

4.8.4 Agency shall protect emergency power shutoff capability from unauthorized activation.

4.9 Emergency Power

4.9.1 Agency shall provide short-term, uninterruptible power supply to allow for an orderly shutdown of the Information System in the event of a primary power source failure.

4.9.2 Agency shall provide long-term, alternate power supply for the Information System that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

4.10 Emergency Lighting

4.10.1 Agency shall employ and maintain automatic emergency lighting that activates in the event of a power disruption and covers emergency exits and evacuation routes within the facility.

4.11 Fire Protection

4.11.1 Agency shall employ and maintain system fire suppression and detection devices/systems for facilities containing concentrations of Information System resources that are supported by an independent energy source.

4.12 Temperature and Humidity Controls

4.12.1 Agency shall maintain appropriate temperature and humidity levels within the facility where the Information System resides.

4.12.2 Agency shall monitor temperature and humidity levels.

4.13 Water Damage Protection

4.13.1 Agency shall protect facilities containing concentrations of Information System resources from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

4.14 Delivery and Removal

4.14.1 Agency shall authorize, monitor, and control defined types of Information System components entering and exiting the facility and shall maintain records of those items.

4.15 Alternate Work Site

4.15.1 Agency shall employ defined security controls at alternate work sites.

4.15.2 Agency shall assess, as feasible, the effectiveness of security controls at alternate work sites.

4.15.3 Agency shall provide a means for Employees to communicate with information security personnel in case of security incidents or problems.

4.16 Location of Information System Components

4.16.1 Agency shall position Information System components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

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 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. 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

7. REVISION HISTORY

Original Effective Date	
Last Review Date	
Revised Date	

8. APPROVALS AND MANAGEMENT COMMITMENT

Effective upon latest signature below.

_____ Date: _____
DoIT Acting Secretary, Kirk Lonbom

_____ Date: _____
Chief Information Security Officer, Chris Hill

_____ Date: _____
DoIT General Counsel, Michael Delcomyn

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 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. 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

7. REVISION HISTORY

Original Effective Date	
Last Review Date	
Revised Date	

8. APPROVALS AND MANAGEMENT COMMITMENT

Effective upon latest signature below.

DoIT Acting Secretary, Kirk Lonbom — Date: 10/8/18

Chief Information Security Officer, Chris Hill — Date: 9/21/18

DoIT General Counsel, Michael Delcomyn — Date: 10/15/18