State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Awareness and Training Policy

1. OVERVIEW

Pursuant to 20 ILCS 450/25, the State of Illinois Department of Innovation & Technology (DoIT) is responsible for the establishment and implementation of cybersecurity awareness and training. This training educates Employees how to safeguard the confidentiality, integrity, and availability of State information technology (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 reduce security risks by educating State of Illinois Employees to help protect and appropriately use IT Resources and data.

3. SCOPE

This Policy applies to all Employees, as defined by the State Officials and Employees Ethics Act (5 ILCS 430/1-5), 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.

4.1 Security Awareness Training (Content Provided by DoIT)

4.1.1 Security awareness training shall be provided by Client Agencies as part of initial training for new Employees.

4.1.2 Security awareness training shall occur when required by Information System changes as deemed necessary by DoIT.

4.1.3 Security awareness training shall occur on an annual basis as required by 20 ILCS 450/25.

4.2 Role-Based Security Training

4.2.1 Role-based security training is special training for Employees with assigned administrative or technical roles and responsibilities involving access to sensitive information, including but not limited to Federal Tax Information, Protected Health Information, and Personally Identifiable Information.

4.2.2 Role-based security training shall be administered by the Client Agency before granting Employees privileged access to the Information System or before Employees begin performing assigned duties.

4.2.3 Role-based security training shall occur on a defined frequency, whenever there is a significant change in the Client Agency's Information System environment or procedures, and whenever an Employee enters a new position that requires additional role-specific training.

4.3 Security Training Records

4.3.1 Client Agencies shall document and monitor individual Information System security training activities, including basic security awareness training and specific Information System security training.

4.3.2 Client Agencies shall retain training records for appropriate periods as defined by law.

5. POLICY COMPLIANCE

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 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

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: 9/22/18

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