State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Access Control

1. OVERVIEW

It is the policy of the State of Illinois to protect State Information Systems against improper or unauthorized access that could result in the compromise of confidentiality, integrity, or availability of State of Illinois information, information technology (IT) assets, or technology-enabled capabilities. The establishment of appropriate and effective access controls helps to prevent accidental damage, disruption, physical tampering, eavesdropping, and other potential incidents. 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 risks posed to State of Illinois Information Systems due to unauthorized or unintentional access, while meeting the access requirements for authorized Users.

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 Account Management

4.1.1 Agency shall identify Information System account types to support its mission and business functions. Account types could include, but are not limited to, group, system, application, guest/anonymous, emergency, and temporary accounts.

4.1.2 Agency account managers shall assign Information System accounts.

4.1.3 Agency shall establish conditions for group and role membership.

4.1.4 Agency shall specify required attributes for authorized Users, group and role membership, and access authorizations.

4.1.5 Accounts shall not be created without specific Agency approval. Information Owners shall approve User accounts, roles, and access levels based on need-to-know rules.

4.1.6 Privileged accounts shall be approved as appropriate by the DoIT-designated Information System Administrator(s).

4.1.7 Agency shall establish standards and/or procedures for creating, enabling, modifying, disabling, and removing Information System accounts for each account type.

4.1.8 Agency shall monitor Information System accounts commensurate with the level of privilege, risk, or other established standards.

4.1.9 Agency shall establish procedures for notifying appropriate account managers when accounts are no longer required or when access level requirements change. Triggers for these notifications

include but may not be limited to: User termination, User transfer, or changes to User job responsibilities.

4.1.10 Agency shall periodically review Information System accounts for compliance with established access rules.

4.2 Access Enforcement

4.2.1 Agency shall have the technical capability to enforce logical access to information and system resources in accordance with access control rules and policies.

4.3 Information Flow Enforcement

4.3.1 DoIT shall authorize and document business and security requirements for information flow between interconnected systems.

4.4 Separation of Duties

4.4.1 Agency shall address the potential for abuse of authorized privileges through the documentation and enforcement of separation of duties. Separation of duties includes but is not limited to: (i) dividing mission functions and Information System support functions; (ii) conducting Information System support functions with different individuals (e.g., system management, programming, and security); and (iii) ensuring that security personnel who administer access control functions do not also administer audit functions.

4.5 Least Privilege

4.5.1 Agency shall employ the principle of least privilege and allow only authorized access for Users (or processing actions on behalf of Users) that is necessary to accomplish assigned tasks.

4.6 Unsuccessful Logon Attempts

4.6.1 Information Systems must automatically lock an account after a maximum number of invalid or unsuccessful logon attempts.

4.7 System Use Notification

4.7.1 Internal Use Systems (State of Illinois Business Applications – Non-Public Use)

- An approved system use notification message or banner shall be displayed that provides privacy and security notices consistent with applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and guidance before granting access to the system. The notification message shall state that:
  - Users are accessing a State of Illinois Information System;
  - unauthorized use of the Information System is prohibited and subject to discipline and criminal and/or civil penalties; and

- use of the Information System indicates consent to monitoring and recording.

4.7.2 Publicly Available Information Systems

- A publicly available Information System shall display system use information that includes a description of authorized uses of the system before granting further access.
- A publicly available Information System shall display references, if any, to applicable monitoring, recording, or auditing that will be present with the use of the publicly available system.

4.7.3 System use notifications shall be retained on the screen until the User- acknowledges the usage conditions and takes explicit actions to log on to or further access the Information System.

4.7.4 Information Systems that are presented strictly for viewing publicly available information may be exempted from the system use notification requirement.

4.8 Session Lock

4.8.1 Information System sessions shall lock after a defined period of inactivity or upon receiving a request from the User.

4.8.2 A session lock shall remain in place until the User reconnects by using established identification and authentication.

4.8.3 Information Systems shall conceal information previously visible on the display with a publicly viewable image.

4.9 Session Termination

4.9.1 Information systems shall automatically terminate a User session after a defined period of inactivity.

4.10 Permitted Actions Without Identification and Authentication

4.10.1 Agency Information System security plans shall document any actions that will be permitted without identification or authentication and provide specific rationale for allowing these actions.

4.11 Remote Access

4.11.1 Usage restrictions and configuration/connection requirements for any planned or in-place remote access to the Information System shall be established and documented by DoIT. Implementation guidance for any remote access to Information Systems shall be developed by DoIT for each type of remote access allowed.

4.11.2 Remote access to Information Systems shall be authorized by the Information Owner prior to allowing such connections. Justification for remote access shall be provided and approved by the Employee's supervisor or designee.

4.11.3 Remote access to the State of Illinois network via virtual private network or similar technologies/connections shall be reviewed and approved by DoIT based on justified business

need as authorized by the User's supervisor. Remote access by third parties must also be approved by DoIT.

4.11.4 Remote access shall be monitored and controlled by DoIT. Cryptographic mechanisms shall be implemented by DoIT for access via virtual private network or similar technologies to further protect the confidentiality and integrity of remote access sessions.

4.11.5 Remote access shall be routed through a limited number of managed access control points by DoIT.

4.11.6 DoIT shall establish additional remote access controls such as geographic boundary, time of day usage, and/or other appropriate controls to further protect the confidentiality and integrity of remote access sessions.

4.12 Wireless Access

4.12.1 Usage restrictions, configuration and connection requirements, and implementation guidance shall be established by DoIT for wireless access to Information Systems and the State of Illinois network.

4.12.2 Wireless access policies and practices shall be authorized by Agency executive management with guidance from DoIT. Agency wireless access to State of Illinois IT assets and infrastructure shall be protected using encryption and authentication of both Users and devices.

4.12.3 Wireless access services provided by DoIT for use by the public and/or visitors shall not be enabled to provide access to the State of Illinois network. Sufficient security controls and technology must be in place to ensure public users have no path through a public network to the State of Illinois network.

4.13 Access Control for Mobile Devices

4.13.1 Usage restrictions and implementation guidance shall be established by DoIT for the use of mobile devices.

4.13.2 Mobile device access to Information Systems must be approved by Agency.

4.13.3 Full-device encryption, or container encryption, shall be utilized by Agency to protect the confidentiality and integrity of information on approved mobile devices.

4.14 Use of External Information Systems

4.14.1 Terms and conditions must be established by Agency prior to allowing external Information Systems to connect to State of Illinois Information Systems. Information System security plans must identify any and all external Information System connections that are planned or in place for the specific Information System. This requirement applies to: (i) any external Information Systems that will access a State of Illinois Information System; and (ii) the processing, storage, or transmission of State of Illinois information with/using external Information Systems.

4.14.2 State of Illinois employees, contractors, or third parties acting on behalf of the State of Illinois are prohibited from using external Information Systems to process, store, or transmit State of Illinois controlled information unless: (i) the Information System has been acquired for specific use by the State of Illinois and has been approved for use by DoIT; (ii) the Information System is being shared as part of a contract, interagency agreement, connection agreement, or other formal agreement; or (iii) the Information System has been explicitly approved by the Chief Information Security Officer.

4.14.3 The use of external systems shall only be approved by the Agency after verifying that the security controls of the external Information System comply with State of Illinois Enterprise Information Security Policies. The Agency authorized to utilize an external Information System must ensure that the external Information System has been properly added to the State of Illinois external Information System portfolio.

4.14.4 External Information System connection agreements shall be retained by the Agency that requires User or Information System access to the external Information System. Any connection agreements must be reviewed and renewed as stipulated in the connection agreements.

4.15 Information Sharing

4.15.1 Information that is restricted under applicable law (e.g., privileged medical information, personally identifiable information, criminal justice information, federal tax information, classified information, and/or other sensitive information) may only be shared following a formal review and authorization. Authorization for the sharing of restricted information may be provided by the Agency's Legal Counsel, the Agency's Privacy Officer, or similar authority.

4.15.2 Information sharing agreements shall be completed by Agency and should, at minimum, define the purpose and justification for the information sharing, the information being shared, the information sharing process, and the procedures for retrieving or disposing of the shared information when the information sharing process is no longer needed.

4.15.3 All information sharing must be in compliance with State of Illinois Enterprise Information Security Policies.

4.15.4 Information Owners shall provide training to authorized Information System Users to assist Users in making appropriate information sharing decisions.

4.16 Publicly Accessible Content

4.16.1 Information Owners shall designate individuals who are authorized to post information onto a publicly available Information System.

4.16.2 Information Owners shall provide training to ensure that authorized Users do not publicly post information that contains non-public information.

4.16.3 Processes shall be established by Agency to review proposed public content prior to public posting to help ensure that non-public information is not included.

4.16.4 Publicly accessible Information Systems shall be reviewed by Agency designated staff for non-public information. Any non-public information discovered will be removed by Agency as soon as reasonably practicable.

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 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 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.