State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy
Identification and Authentication

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for the establishment and implementation of appropriate identification and authentication controls that safeguard the confidentiality, integrity, and availability of Information Systems. This Policy alleviates security risks by managing risks from User access and authentication to Information Systems through the establishment of effective identification and authentication processes. 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 creating processes and procedures for securely identifying and authenticating State of Illinois 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

4.1 Identification and Authentication

4.1.1 The Information System shall uniquely identify and authenticate the User.

4.2 Device Identification and Authentication

4.2.1 The Information System shall uniquely identify and authenticate State of Illinois devices before establishing a network connection.

4.3 Identifier Management

4.3.1 The Information System shall receive authorization from authorized personnel to assign an individual, group, role, or device identifier.

4.3.2 The Information System shall select and assign an identifier that identifies an individual, group, role, or device.

4.3.3 The Information System shall prevent the reuse of identical identifiers for a defined time period.

4.3.4 The Information System shall disable the identifier after a defined time period ofinactivity.

4.4 Authenticator Management

4.4.1 The Information System shall verify, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

4.4.2 The Information System shall establish initial authenticator content for authenticators defined by the Agency.

4.4.3 The Information System shall ensure that authenticators have sufficient strength of mechanism for their intended use.

4.4.4 The Information System shall establish and implement administrative procedures for distributing initial authenticators, for handling lost/compromised or damaged authenticators, and for revoking authenticators.

4.4.5 The Information System shall change default content of authenticators prior to Information System installation.

4.4.6 The Information System shall contain minimum and maximum lifetime restrictions and reuse conditions for authenticators.

4.4.7 The Information System shall change/refresh authenticators on a defined time period.

4.4.8 The Information System shall protect authenticator content from unauthorized disclosure and modification.

4.4.9 The Information System shall require Users to take, and have devices implement, specific security safeguards to protect authenticators.

4.4.10 The Information System shall change authenticators for group/role accounts when membership to those accounts changes.

4.5 Authenticator Feedback

4.5.1 The Information System shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

4.6 Cryptographic Module Authentication

4.6.1 The Information System shall implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for such authentication.

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 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.