160 – Identification and Authentication Standard

Purpose

The Identification and Authentication Standard provides documentation of the minimum requirements for verification of unique identity(s) and authentication of the identity of individuals, processes, and/or devices prior to accessing State IT systems, system environments, and services.

This standard is applicable to the following:

- Identification and Authentication Policy (IA-01); and,
- Access Control Policy and Standard (AC-01, 100 Access Control)

Standard

This standard uses the NIST SP 800-53 Rev. 5 framework as the guideline to establish control objectives to address a diverse set of security and privacy requirements. Not all controls within NIST SP 800-53 Rev. 5 may be selected for the Statewide baseline policies and standards. Agencies must categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately. This standard uses Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. At a minimum, all low controls are selected, and certain moderate controls are selected. Agencies are to reflect their controls through the annual reporting process to DOA-DET.

Executive Branch Agencies are to develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. Implementation of the standard controls within this document can be (1) a common (inheritable) control, (2) a system-specific control, or (3) a hybrid control. The control implementation defines the scope of applicability for the control, the shared nature or inheritability of the control, and the responsibility for control development, implementation, assessment, and authorization. Agencies should consider the following for inclusion in their policies, procedures, or processes:

Identification and Authentication (Agency Users) (IA-2):

- Uniquely identifying and authenticating Agency users and associating that unique identification with processes acting on behalf of those users.

Multifactor Authentication to Privileged Accounts (IA-2(1)):

- Implementing multi-factor authentication for access to privileged accounts.

Multifactor Authentication to Non-Privileged Accounts (IA-2(2)):

- Implementing multi-factor authentication for access to non-privileged accounts.

Access to Accounts – Replay Resistant (IA-2(8)):

- Implementing replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

Device Identification and Authentication (IA-3):

- Uniquely identifying and authentication Agency-defined devices and/or types of devices before establishing a connection (i.e., local, remote, or network connection).

Identifier Management (IA-4):

- Managing system identifiers by:
  - Receiving authorization from Agency-defined personnel/roles to assign an individual, group, role, service, or device identifier;
  - Selecting an identifier that identifies an individual, group, role, service, or device;
  - Assigning the identifier to the intended individual, group, role, service, or device; and
  - Preventing reuse of identifiers for an Agency-defined time period.

Identifier User Status (IA-4(4)):

- Managing individual identifiers by uniquely identifying each individual Agency-defined characteristic identifying individual status. (Characteristics that identify the status of individuals include contractors, foreign nationals, and non-organizational users.)

Authenticator Management (IA-5):

- Managing system authentications by:
  - Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
  - Establishing initial authenticator content for any authenticators issued by the agency;
  - Ensuring that authenticators have sufficient strength of mechanism for their intended use;
  - Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
  - Changing default authenticators prior to first use;
  - Changing or refreshing authenticators based on an Agency-defined time period by authenticator type or when Agency-defined events occur;
  - Protecting authenticator content from unauthorized disclosure and modification;
  - Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
  - Changing authenticators for group or role accounts when membership to those accounts change.

Password-Based Authentication (IA-5(1)):

- Password-based authentication controls are included in the 161 Password Standard.

Public Key-Based Authentication (IA-5(2)):

- For public-key based authentication:
  - Enforce authorized access to the corresponding private key; and
  - Map the authenticated identity to the account of the individual or group; and
- When public key infrastructure (PKI) is used:
  - Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
  - Implement a local cache of revocation data to support path discovery and validation.

Protection of Authenticators (IA-5(6)):

- Protecting authenticators commensurate with the security category of the information to which the authenticator permits access.

Authenticator Feedback (IA-6):

- Obscuring feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Cryptographic Module Authentication (IA-7):

- Implementing mechanisms for authentication to a cryptographic module that meets the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

Identification and Authentication (Non-Agency Users) (IA-8):

- Uniquely identifying and authenticating non-agency users or processes acting on behalf of non-agency users.

Re-authentication (IA-11):

- Requiring users to re-authenticate when an Agency-defined circumstance or situation occurs requiring re-authentication (i.e., when roles, authenticators, or credentials change, when security categories or systems change, when the execution of privileged functions occurs, after a fixed time period, or periodically).

Identity Proofing (IA-12):

- Identity proofing users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.

- Resolving user identities to a unique individual; and
- Collecting, validating, and verifying identity evidence.

Identity Evidence (IA-12(2)):

- Requiring evidence of individual identification be presented to the registration authority.

Identity Evidence Validation and Verification (IA-12(3)):

- Requiring that the presented identity evidence be validated and verified through an Agency-defined method of validation and verification.

Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
State information - Any information that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.
State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to: network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed the agency.

Exception Process

Exceptions to any Executive Branch Agencies Security Policies, Procedures or Standards must follow the Executive Branch Agencies Exception Procedure.

Document History/Owner

This standard was developed as required by the State of Wisconsin Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to the DET Bureau of Security. As such, the DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
1.0	10/15/18	Submitted to and approved by the IT Executive Steering Committee	Reviewer: ITESC Author: DOA/DET	10/15/18
1.0	10/29/19	Reviewed with Agency Security Officers and feedback collected. Planning for making revisions.	Bureau of Security	10/29/19
2.0	11/03/20	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	11/11/20
3.0	06/24/22	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	06/24/22
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				

Authorized and Approved by:

Alan Greenberg, CISO

DocuSigned by:
Alan Greenberg
7062227F849B429...

7/8/2022 | 1:55 PM CDT

Print/Type
Title

Signature

Date