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 3-7 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 quarterly 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. Some agencies will have specific regulatory requirements that they must adhere to that go beyond what other agencies would need to adhere to. 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.

This standard is divided into two sections of controls. **Section One** includes the minimum baseline controls that Executive Branch agencies are to adhere to. **Section Two** includes additional controls for agencies that are subject to regulatory requirements. The list in Section Two is not all-inclusive. Agencies may have additional controls they must adhere to that are not listed here.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (IA-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:

- An identification and authentication policy that:
  - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
  - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
- Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and
- Review and update the current identification and authentication:
  - Policy on an agency-defined frequency; and
  - Procedures on an agency-defined frequency.

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

- Uniquely identify and authenticate agency users and associate that unique identification with processes acting on behalf of those users.

Identification and Authentication | Multi-factor Authentication to Privileged Accounts (IA-2(1)):

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

Identification and Authentication (Agency Users) | Multi-factor Authentication to Non-Privileged Accounts (IA-2(2)):

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

Identification and Authentication (Agency Users) | Access to Accounts – Replay Resistant (IA-2(8)):

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

Identification and Authentication (Agency Users) | Acceptance of PIV Credentials (IA-2(12)):

- Accept and electronically verify Personal Identity Verification-compliant credentials.

Device Identification and Authentication (IA-3):

- Uniquely identify and authenticate agency-defined devices and/or types of devices before establishing a connection (i.e., local, remote, or network connection).

Identifier Management (IA-4):

- Manage system identifiers by:
  - Receiving authorization from designated agency 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 Management | Identifier User Status (IA-4(4)):

- Manage individual identifiers by uniquely identifying each individual as 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):

- Manage 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.

Authenticator Management | Password-Based Authentication (IA-5(1)):

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

Authenticator Management | 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.

Authenticator Management | Protection of Authenticators (IA-5(6)):

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

Authenticator Feedback (IA-6):

- Obscure 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):

- Implement mechanisms for authentication to a cryptographic module that meet 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 identify and authenticate non-agency users or processes acting on behalf of non-agency users.

Identification and Authentication (Non-Agency Users) | Acceptance of PIV Credentials from Other Agencies (IA-8(1)):

- Accept and electronically verify Personal Identity Verification-compliant credentials from other agencies.

Identification and Authentication (Non-Agency Users) | Acceptance of External Authenticators (IA-8(2)):

- Accept only external authenticators that are NIST-compliant; and
- Document and maintain a list of accepted external authenticators.

Identification and Authentication (Non-Agency Users) | Use of Defined Profiles (IA-8(4)):

- Conform to agency-defined identity management profiles for identity management.

Re-authentication (IA-11):

- Require 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 proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines.
- Resolve user identities to a unique individual; and
- Collect, validate, and verify identity evidence.

Identity Proofing | Supervisor Authorization (IA-12(1)):

- Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

Identity Proofing | Identity Evidence (IA-12(2)):

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

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

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

Identity Proofing | Address Confirmation (IA-12(5)):

- Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies must adhere to the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Identification and Authentication (Agency Users) | Individual Authentication with Group Authentication (IA-2(5)):

- When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Authenticator Management | Change Authenticators Prior to Delivery (IA-5(5)):

- Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.

Authenticator Management | No Embedded Unencrypted Static Authenticators (IA-5(7)):

- Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.

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 Agency's Security Policies or Standards must follow the Executive Branch Risk 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	10/29/19	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
4.0	07/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/Enterprise IT Author: DOA/DET/BOS	07/31/23
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:

Trina Zanow, CIO

DocuSigned by:
Trina Zanow
A41B57ECEC77402...

7/31/2023 | 4:07 PM CDT

Print/Type
Title

Signature

Date