100 – Access Control Standard

Purpose

The Access Control Standard provides documentation of the minimum Access Control requirements for access to Executive Branch Agencies Information Technology (IT) systems and system environments.

This standard is intended to facilitate the attainment of the Access Control Policy, the Configuration Management Policy, the Password Standard, Personnel Screening Standard, and associated Information Technology (IT) Security Policy objectives (AC-1, CM-1).

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 as a baseline. 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 (AC-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - An access control 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 access control policy and the associated access controls;
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the access control policy and procedures; and
- Review and update the current access control:
    - Policy on an agency-defined frequency; and
    - Procedures on an agency-defined frequency.

Account Management (AC-2):

- Define and document the types of accounts allowed and specifically prohibited for use within the system. (Examples of account types include individual, shared, group, system, guest, emergency, developer, temporary, and service);
- Assign account managers;
- Require conditions for group and role membership;
- Specify:
    - Authorized users of the system;
    - Group and role membership; and
    - Access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Require approvals by agency-defined personnel or roles for requests to create accounts;
- Create, enable, modify, disable, and remove accounts in accordance with agency-defined policies, procedures, prerequisites, and criteria;
- Monitor the use of accounts;
- Notify account managers and appropriate agency personnel or roles:
    - Immediately when accounts are no longer required;
    - Immediately when users are terminated or transferred; and
    - Immediately when system usage or need-to-know changes for an individual;
- Authorize access to the system based on:
    - A valid access authorization;
    - Intended system usage; and
    - Agency-defined attributes (as required);
- Review accounts for compliance with account management requirements on an agency-defined frequency;
- Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
- Align account management processes with personnel termination and transfer processes.

Account Management | Automated System Account Management (AC-2(1)):

- Support the management of system accounts using automated mechanisms.

Account Management | Automated Temporary and Emergency Account Management (AC-2(2)):

- Automatically remove/disable temporary and emergency accounts after an agency-defined time period for each type of account.

Account Management | Disable Accounts (AC-2(3)):

- Disable accounts within an agency-defined time period when the accounts:
  - Have expired;
  - Are no longer associated with a user or individual;
  - Are in violation of agency policy; or
  - Have been inactive for a maximum of 120 days.

Account Management | Automated Audit Actions (AC-2(4)):

- Automatically audit account creation, modification, enabling, disabling, and removal actions.

Account Management | Inactivity Logout (AC-2(5)):

- Require that users log out when there is an agency-defined time period of expected inactivity or before leaving the system unattended.

Account Management | Disable Accounts for High-Risk Users (AC-2(13)):

- Disable accounts of individuals immediately upon discovery of significant security or privacy risks.

Access Enforcement (AC-3):

- Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Access Enforcement | Individual Access (AC-3(14)):

- Provide mechanisms to enable individuals to have access to agency-defined elements of their personally identifiable information.

Information Flow Enforcement (AC-4):

- Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on information flow control policies.

Separation of Duties (AC-5):

- Identify and document duties of individuals requiring separation; and
- Define system access authorizations to support separation of duties.

Least Privilege (AC-6):

- Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned agency tasks.

Least Privilege | Authorize Access to Security Functions (AC-6(1)):

- Authorize access for individuals or roles to:
  - Security functions deployed in hardware, software, and firmware; and
  - Agency-defined security-relevant information.

Least Privilege | Non-Privileged Access for Non-Security Functions (AC-6(2)):

- Require that users of system accounts (or roles) with access to agency-defined security functions or security-relevant information use non-privileged accounts or roles, when accessing non-security functions.

Least Privilege | Privileged Accounts (AC-6(5)):

- Restrict privileged accounts on the system to agency-defined personnel or roles.

Least Privilege | Review of User Privileges (AC-6(7)):

- Review on an agency-defined frequency the privileges assigned to roles or classes of users to validate the need for such privileges; and
- Reassign or remove privileges, if necessary, to correctly reflect agency mission and business needs.

Least Privilege | Log Use of Privileged Functions (AC-6(9)):

- Log the execution of privileged functions.

Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions (AC-6(10)):

- Prevent non-privileged users from executing privileged functions.

Unsuccessful Logon Attempts (AC-7):

- Enforce a limit of three (3) consecutive invalid logon attempts by a user within a 120-minute period.
- Automatically lock the account when the maximum number of unsuccessful attempts is exceeded.

System Use Notification (AC-8):

- Display an agency-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
  - Users are accessing a State of Wisconsin information system;
  - System usage may be monitored, recorded, and subject to audit;
  - Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
  - Use of the system indicates consent to monitoring and recording;
- Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
- For publicly accessible systems:

- Display system use information before granting further access to the publicly accessible system;
- Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
- Include a description of the authorized uses of the system.

Device Lock (AC-11):

- Prevent further access to the system by initiating a device lock after 15 minutes of inactivity; requiring the user to initiate a device lock before leaving the system unattended; and
- Retain the device lock until the user reestablishes access using established identification and authentication procedures.

Device Lock | Pattern-Hiding Displays (AC-11(1)):

- Cancel, via the device lock, information previously visible on the display with a publicly viewable image.

Session Termination (AC-12):

- Automatically terminate a user session after agency-defined conditions or trigger events requiring session disconnect. Conditions or trigger events that require automatic termination of the session include agency-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on system use.

Permitted Actions without Identification or Authentication (AC-14):

- Identify user actions that can be performed on the system without identification or authentication consistent with agency mission and business functions; and
- Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Remote Access (AC-17):

- See 101 Access Control for Remote Access Standard for controls related to remote access.

Wireless Access (AC-18):

- See 102 Access Control for Wireless Access Standard for controls related to wireless access.

Access Control for Mobile Devices (AC-19):

- See 103 Access Control for Mobile Device Security Standard for controls related to mobile devices.

Use of External Systems (AC-20):

- Establish terms and conditions and/or identify controls asserted to be implemented on external systems, consistent with the trust relationships established with other organizations owning,

operating, and/or maintaining external systems, allowing authorized individuals to:
    - Access the system from external systems; and
    - Process, store, or transmit agency-controlled information using external systems; or
- Prohibit the use of agency-defined types of external systems.

Use of External Systems | Limits of Authorized Use (AC-20(1)):

- Permit authorized individuals to use an external system to access the system or to process, store, or transmit agency-controlled information only after:
    - Verification of the implementation of controls on the external system as specified in the agency's security and privacy policies and security and privacy plans; or
    - Retention of approved system connection or processing agreements with the agency entity hosting the external system.

Use of External Systems | Portable Storage Devices – Restricted Use (AC-20(2)):

- Restrict the use of agency-controlled portable storage devices by authorized individuals on external systems using agency-defined restrictions.

Information Sharing (AC-21):

- Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for agency-defined information sharing circumstances where user discretion is required; and
- Employ automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

Publicly Accessible Content (AC-22):

- Designate individuals authorized to make information publicly accessible;
- Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
- Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and
- Review the content on the publicly accessible system for nonpublic information on an agency-defined frequency and removing such content, if discovered.

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.

Account Management | Privileged User Accounts (AC-2(7)):

- Establish and administer privileged user accounts in accordance with a role-based scheme or an attribute-based access scheme;
- Monitor privileged role or attribute assignments;
- Monitor changes to roles or attributes; and
- Revoke access when privileged role or attribute assignments are no longer appropriate.

Account Management | Restrictions On Use of Shared and Group Accounts (AC-2(9)):

- Only permit the use of shared and group accounts that meet agency-defined conditions for establishing shared and group accounts.

Account Management | Account Monitoring for Atypical Usage (AC-2(12)):

- Monitor system accounts for atypical usage; and
- Report atypical usage of system accounts to appropriate agency personnel or roles.

Access Enforcement | Controlled Release (AC-3(9)):

- Release information outside of the system only if:
    - The receiving system or system component provides agency-defined controls; and
    - Agency-defined controls are used to validate the appropriateness of the information designated for release.

Concurrent Session Control (AC-10):

- Limit the number of concurrent sessions for each agency-defined account and/or account type to an agency-defined number.

Session Termination | User-Initiated Logouts (AC-12(1)):

- Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to agency-defined information resources.

Use of External Systems | Non-Organizationally Owned Systems – Restricted Use (AC-20(3)):

- Restrict the use of non-organizationally owned systems or system components to process, store, or transmit agency information using agency-defined restrictions.

Data Mining Protection (AC-23):

- Employ agency-defined data mining prevention and detection techniques for agency-defined data storage objects to detect and protect against unauthorized data mining.

Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.

State information - Any information/data 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 by the agency.

Identified Account Types - Include: Individual, privileged (administrative and default privileged), shared, service, emergency, and temporary accounts (temporary and guest wireless account) (AC-2).

Control Baseline – A control baseline is a collection of controls assembled to address the protection needs of a group, organization, or community of interest. It provides a generalized set of controls that represent a starting point for the subsequent tailoring activities that are applied to the baseline to produce a targeted or customized security and privacy solution for the entity that the baseline is intended to serve.

Exception Process

Exceptions to any Executive Branch Agency's Security Policies or Standards must follow the Executive Branch Risk Exception Procedure.

Document History and Ownership

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 revised, updated, or retired.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, 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: ITESC Author: DOA/DET	06/24/22
4.0	07/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and 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
A11B57ECEC77402...

7/31/2023 | 4:07 PM CDT

Print/Type Title | Signature | Date