# 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. 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:

### Account Management (AC-2):

- Defining and documenting 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);
- Assigning account managers;
- Requiring Agency-defined prerequisites and criteria for group and role membership;
- Specifying:
    - Authorized users of the system;
    - Group and role membership; and
    - Access authorizations (i.e., privileges) and Agency-defined attributes (as required) for each account;
- Requiring approvals by Agency-defined personnel/roles for requests to create accounts;
- Creating, enabling, modifying, disabling, and removing accounts in accordance with Agency-

defined policy, procedures, prerequisites, and criteria;

- Monitoring the use of accounts;
- Notifying account managers and Agency-defined personnel/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;
- Authorizing access to the system based on:
  - A valid access authorization;
  - Intended system usage; and
  - Agency-defined attributes (as required);
- Reviewing accounts for compliance with account management requirements annually;
- Establishing and implementing a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
- Aligning account management process with personnel termination and transfer processes.

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

- Supporting the management of system accounts using Agency-defined automated mechanisms.

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

- Automatically removing/disabling temporary and emergency accounts after an Agency-defined time period for each type of account.

### Disable Accounts (AC-2(3)):

- Disabling 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.

### Automated Audit Actions (AC-2(4)):

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

### Inactivity Logout (AC-2(5)):

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

### Disable Accounts for High-Risk Users (AC-2(13)):

- Disabling accounts of individuals immediately upon discovery of Agency-defined significant security or privacy risks.

## Access Enforcement (AC-3):

- Enforcing approved authorizations for logical access to information and system resources

in accordance with applicable access control policies.

## Information Flow Enforcement (AC-4):

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

## Separation of Duties (AC-5):

- Identifying and documenting Agency-defined duties of individuals requiring separation; and
- Defining system access authorizations to support separation of duties.

## Least Privilege (AC-6):

- Employing 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.

### Authorize Access to Security Functions (AC-6(1)):

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

### Non-Privileged Access for Non-security Functions (AC-6(2)):

- Requiring 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.

### Privileged Accounts (AC-6(5)):

- Restricting privileged accounts on the system to Agency-defined personnel or roles.

### Review of User Privileges (AC-6(7)):

- Annually reviewing the privileges assigned to roles or classes of users to validate the need for such privileges. Access to privileged accounts must be reviewed every six months (minimally) to determine whether the account is still required, and access remains appropriate;
- Reassigning or removing privileges, if necessary, to correctly reflect agency mission and business needs.

### Log Use of Privileged Functions (AC-6(9)):

- Logging the execution of privileged functions.

### Prohibit Non-Privileged Users from Executing Privileged Functions (AC-6(10)):

- Preventing non-privileged users from executing privileged functions.

## Unsuccessful Logon Attempts (AC-7):

- Enforcing a limit of three (3) consecutive invalid logon attempts by a user within a 120-minute period.

## System Use Notification (AC-8):

- Displaying 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;
- Retaining 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.

## Device Lock (AC-11):

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

### Pattern-Hiding Displays (AC-11(1)):

- Cancelling, 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):

- Identifying Agency-defined user actions that can be performed on the system without identification or authentication consistent with agency mission and business functions; and
- Documenting and providing 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):

- Establishing Agency-defined terms and conditions and/or identifying Agency-defined 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
- Prohibiting the use of Agency-defined types of external systems.

### Limits of Authorized Use (AC-20(1)):

- Permitting 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 plan; or
    - Retention of approved system connection or processing agreements with the agency entity hosting the external system.

### Portable Storage Devices – Restricted Use (AC-20(2)):

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

## Information Sharing (AC-21):

- Enabling 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
- Employing Agency-defined automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

### Publicly Accessible Content (AC-22):

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

## 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 Account and Guest Wireless Account) (AC-2).

## Exception Process

Exceptions to any Executive Branch Agencies Security Policies, Procedures or Standards must follow the Executive Branch Agencies 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 | 10/15/18 | Submitted to and approved by the IT Executive Steering Committee | Reviewer: ITESC<br>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<br>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<br>Author: DOA/DET | 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