



STATE OF WISCONSIN

DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

101 - Access Control for Remote Access Standard

Purpose

This standard is intended to facilitate the attainment of the Access Control Policy and associated Information Technology (IT) Security Policy objectives.

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 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

Remote Access (AC-17):

- Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
- Authorize each type of remote access to the system prior to allowing such connections.

Remote Access | Monitoring and Controlling (AC-17(1)):

- Employ automated mechanisms to monitor and control remote access methods.



STATE OF WISCONSIN

DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

Remote Access | Protection of Confidentiality and Integrity Using Encryption (AC-17(2)):

- For systems and data identified as moderate risk, implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Remote Access | Managed Access Control Points (AC-17(3)):

- Route remote access through authorized and managed network access control points.

Remote Access | Privileged Commands and Access (AC-17(4)):

- Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and following agency needs; and
- Document the rationale for remote access in the security plan for the system.

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.

Remote Access | Disconnect or Disable Access (AC-17(9)):

- Provide the capability to disconnect or disable remote access to the system within an agency-defined time period.

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.

DET/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.



STATE OF WISCONSIN DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

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 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.



**STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION**

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

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
Signature

7/31/2023 | 4:07 PM CDT

Print/Type
Title

Date