



# STATE OF WISCONSIN

## DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor  
Kathy Blumenfeld, Secretary  
Trina Zanow, Division Administrator  
Effective Date: 07/01/2022

## 102 - Access Control for Wireless 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 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. 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. Agencies should consider the following for inclusion in their policies, procedures, or processes:

### Wireless Access (AC-18):

- Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access.
- Authorize each type of wireless access to the system prior to allowing such connections.

### Authentication and Encryption (AC-18(1)):

- Protecting wireless access to the system using authentication of users or devices and encryption.



## 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 by 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 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: 07/01/2022

Table with 5 columns: Version #, Revision or Review Date, Description of Change(s), Reviewer/Author, Date Approved. Contains 4 rows of revision history and a note at the bottom.

Authorized and Approved by:

Alan Greenberg, CISO

DocuSigned by: Alan Greenberg

7/8/2022 | 1:55 PM CDT

Print/Type Title

Signature

Date