210 - Security Planning Standard

Purpose

The Information Technology (IT) Security Planning standard provides documentation to achieve compliance with the IT Security Planning Policy.

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 3-12 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 includes the minimum baseline controls that Executive Branch agencies are to adhere to. Agencies may have additional controls they must adhere to that are not listed here.

BASELINE CONTROLS

Policy and Procedures (PL-1):
- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A planning 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 planning policy and the associated planning controls;

STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION
Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

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

System Security and Privacy Plans (PL-2):

- Develop security and privacy plans for the system that:

    - Are consistent with the enterprise architecture;

    - Explicitly define the constituent system components;

    - Describe the operational context of the system in terms of mission and business processes;

    - Identify the individuals that fulfill system roles and responsibilities;

    - Identify the information types processed, stored, and transmitted by the system;

    - Provide the security categorization of the system, including supporting rationale;

    - Describe any specific threats to the system that are of concern to the agency;

    - Provide the results of a privacy risk assessment for systems processing personally identifiable information.

    - Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

    - Provide an overview of the security and privacy requirements for the system;

    - Identify any relevant control baselines or overlays, if applicable;

    - Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;

    - Include risk determinations for security and privacy architecture and design decisions;

    - Include security- and privacy-related activities affecting the system that require planning and coordination with authorized agency personnel; and

    - Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

- Distribute copies of the plans and communicate subsequent changes to the plans to authorized agency personnel;

- Review the plans on an agency-defined frequency;

- Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

- Protect the plans from unauthorized disclosure and modification.

STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION
Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

Rules of Behavior (PL-4):

- Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy (e.g., Acceptable Use Agreement);
- Receive a documented acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
- Review and update the rules of behavior on an agency-defined frequency.
- Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated.

Rules of Behavior | Social Media and External Site/Application Usage Restrictions (PL-4(1)):

- Include in the rules of behavior, restrictions on:
  - Use of social media, social networking sites, and external sites/applications;
  - Posting agency information on public websites; and
  - Use of agency-provided identifies (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

Security and Privacy Architectures (PL-8):

- Develop security and privacy architectures for the system that:
  - Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of agency information;
  - Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
  - Describe how the architectures are integrated into and support the enterprise architecture; and
  - Describe any assumptions about, and dependencies on, external systems and services;
- Review and update the architecture annually to reflect changes in the enterprise architecture; and
- Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, agency procedures, and procurements and acquisitions.

Central Management (PL-9):

- Centrally manage agency-defined controls and related processes.

Baseline Selection (PL-10):

- Select a control baseline for the system.

STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION
Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

Baseline Tailoring (PL-11):

- Tailor the selected control baseline by applying specified tailoring actions.

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.

Information Asset – All State information and State information systems and environments.

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 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: 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	08/01/23
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

Print/Type
Title

DocuSigned by:

Trina Zanow

Signature A11B57E6EC77402...

8/1/2023 | 1:49 PM CDT

Date