220 – Personnel Security Standard

Purpose

The Personnel Security standard provides documentation of the requirements to achieve compliance with the Personnel Security Policy and other applicable policies, procedures, and/or standards. This standard is applicable to all Executive Branch agency employees, interns, contractors, and/or vendors with access to State IT systems and system environments.

Standard

Based on NIST SP 800-53 Rev. 5, DET's Standards address a diverse set of security and privacy requirements. As a currently established baseline for implementation, DOA utilizes all low level, and selected moderate level controls in support of its security posture initiatives. Agencies shall categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately as defined by Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. Agencies shall update DET on the status of their baseline control implementation through the reporting and monitoring process.

Executive Branch Agencies shall develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. **Note:** Some agencies have specific regulatory requirements to follow that go above and beyond the requirements for other agencies. 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 contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Policy and Procedures (PS-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A personnel security policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
  - Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls.
- Designate appropriate agency personnel to manage the development, documentation, and

dissemination of the personnel security policy and procedures.

- Review and update the current personnel security:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Position Risk Designation (PS-2):

- Follow agency policies, procedures, and standards for assigning risk (or classification) and hiring employees, interns, and contractors.

Personnel Screening (PS-3):

- All State employees, interns, and contractors must have personnel (citizen/residency reference checks) and security (background checks) screenings prior to employment.
- Individuals who work at consolidated datacenters must have an FBI fingerprint background check initiated prior to accessing areas with sensitive or confidential areas.
- Security background checks are required at a minimum of every 5 years.

Personnel Termination (PS-4):

- Upon termination of individual employment:
  - Disable system access within an agency-defined time period.
  - Terminate or revoke any authenticators or credentials with the individual.
  - Conduct exit interviews, when applicable.
  - Retrieve all security-related organizational system-related property.
  - Retain access to agency information and systems formerly controlled by the terminated individual.

Personnel Transfer (PS-5):

- Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the agency.
- Initiate agency-defined transfer or reassignment actions within an agency-defined period of time following the formal transfer.
- Modify access authorizations as needed to correspond with any changes in operational needs due to reassignment or transfer.
- Notify agency personnel or roles within an agency-defined time period.

Access Agreements (PS-6):

- Develop and document access agreements for agency systems.
- Review and update access agreements on an agency-defined frequency.
- Verify that individuals requiring access to agency information and systems:
  - Sign appropriate access agreements prior to being granted access.
  - Re-sign access agreements to maintain access to agency systems when agreements have been updated or required by an agency-defined frequency.

External Personnel Security (PS-7):

- Establish personnel security requirements, including security roles and responsibilities for external

providers.

- Require external providers to comply with personnel security policies and procedures established by the agency.
- Document personnel security requirements.
- Require external providers to notify agency personnel or roles of any personnel transfers or terminations of external personnel who possess State information (including credentials/badges) or who have system privileges within an agency-defined time period.
- Monitor provider compliance with personnel security requirements.

Personnel Sanctions (PS-8):

- Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures.
- Notify designated agency personnel within an agency-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Position Descriptions (PS-9):

- Incorporate security and privacy roles and responsibilities into agency position descriptions.

Definitions

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

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 Agency's Security Policies or Standards shall 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 Wis. Stat. § 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.

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
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 and Enterprise IT Author: DOA/DET/BOS	08/01/23
5.0	7/2/24	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	7/30/24
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:

Troy Stairwalt, State of Wisconsin Chief Information Security Officer

DocuSigned by:
Troy Stairwalt
DEEB606FC2524A8...

7/31/2024 | 4:05 PM CDT

Print/Type Signature Date
Title