DocuSign Envelope ID: DFC99A55-D2EF-48B7-B9A7-F946B6DA45C1

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

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 3-14 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 (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; and
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
  - Procedures to facilitate the implementation of the personnel security policy and the

DocuSign Envelope ID: DFC99A55-D2EF-48B7-B9A7-F946B6DA45C1

associated personnel security controls;

- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the personnel security policy and procedures; and
- Review and update the current personnel security:
  - Policy on an agency-defined frequency; and
  - 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; and
- 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; and
  - 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; and
- 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; and
- Verify that individuals requiring access to agency information and systems:
  - Sign appropriate access agreements prior to being granted access; and
  - Re-sign access agreements to maintain access to agency systems when agreements have been

DocuSign Envelope ID: DFC99A55-D2EF-48B7-B9A7-F946B6DA45C1

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; and
- 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; and
- 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.

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 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

DocuSign Envelope ID: DFC99A55-D2EF-48B7-B9A7-F946B6DA45C1

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.

DocuSign Envelope ID: DFC99A55-D2EF-48B7-B9A7-F946B6DA45C1

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

DocuSigned by:
Trina Zanow
1857E0EC77402...

8/1/2023 | 1:49 PM CDT

Print/Type
Title

Signature

Date