500 – Program Management Standard

Purpose

The purpose of the Program Management standard is to facilitate the attainment of the Program Management Policy and associated Information Technology (IT) Security objectives.

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 is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Information Security Program Plan (PM-1):

- Develop and disseminate an agency-wide information security program plan that:
  - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
  - Includes the identification and assignment of roles, responsibilities, management commitment, coordination among agency entities, and compliance.
  - Reflects the coordination among agency entities responsible for information security.

- Is approved by a senior official with responsibility and accountability for the risk being incurred to agency operations (including mission, functions, image, and reputation), agency assets, individuals, other agencies, and the State.

- Review and update the agency-wide information security program plan on an agency-defined frequency and following agency-defined events.
- Protect the information security program plan from unauthorized disclosure and modification.

Plan of Action and Milestones Process (PM-4):

- Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated agency systems:
  - Are developed and maintained.
  - Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to agency operations and assets, individuals, other organizations, and the State.
  - Are reported in accordance with established reporting requirements.
- Review plans of action and milestones for consistency with the agency risk management strategy and organization-wide priorities for risk response actions.

System Inventory (PM-5):

- Develop and update on an agency-defined frequency an inventory of agency systems.

System Inventory | Inventory of Personally Identifiable Information (PM-5(1)):

- Establish, maintain, and update on an agency-defined frequency an inventory of all systems, applications, and projects that process personally identifiable information.

Enterprise Architecture (PM-7):

- Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to agency operations and assets, individuals, other organizations, and the State.

Risk Management Strategy (PM-9):

- Develop a comprehensive strategy to manage:
  - Security risk to agency operations and assets, individuals, other organizations, and the State associated with the operation and use of agency systems.
  - Privacy risk to individuals resulting from the authorized processing of personally identifiable information.
- Implement the risk management strategy consistently across the agency.
- Review and update the risk management strategy every three (3) years or as required, to address agency changes.

Authorization Process (PM-10):

- Manage the security and privacy state of agency systems and the environments in which those systems operate through authorization processes.

- Designate individuals to fulfill specific roles and responsibilities within the agency risk management process.
- Integrate the authorization process into an agency-wide risk management program.

Mission and Business Process Definition (PM-11):

- Define agency mission and business processes with consideration for information security and privacy and the resulting risk to agency operations, agency assets, individuals, other organizations, and the State.
- Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes.
- Review and revise the mission and business process on an agency-defined frequency.

Testing, Training, and Monitoring (PM-14):

- Implement a process for ensuring that agency plans for conducting security and privacy testing, training, and monitoring activities associated with agency systems:
    - Are developed and maintained.
    - Continue to be executed.
- Review testing, training, and monitoring plans for consistency with the agency risk management strategy and agency-wide priorities for risk response actions.

Privacy Program Plan (PM-18):

- Develop and disseminate an agency-wide privacy program plan that provides an overview of the agency's privacy program, and:
    - Includes a description of the structure of the privacy program and the resources dedicated to the privacy program.
    - Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements.
    - Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities.
    - Describes management commitment, compliance, and the strategic goals and objectives of the privacy program.
    - Reflects coordination among agency entities responsible for the different aspects of privacy.
    - Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to agency operations (including mission, functions, image, and reputation), agency assets, individuals, other organizations, and the State.
- Update the plan on an agency-defined frequency to address changes in state and federal privacy laws and policy and agency changes and problems identified during plan implementation or privacy control assessments.

Minimization of Personally Identifiable Information Used in Testing, Training, and Research (PM-25):

- Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research.

- Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes.
- Authorize the use of personally identifiable information when such information is required for internal testing, training, and research.
- Review and update policies and procedures on an annual basis.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also 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.

Information Security and Privacy Resources (PM-3):

- Include the resources needed to implement the information security and privacy programs in capital management planning and investment requests and document all exceptions to the requirement.
- Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, and standards.
- Make available for expenditure, the planned information security and privacy resources.

Insider Threat Program (PM-12):

- Implement an insider threat program that includes a cross-discipline insider incident handling team.

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.

DOA 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 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	7/14/23	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
[illegible]2524A8...

7/31/2024 | 4:05 PM CDT

Print/Type
Title

Signature

Date