250 – System and Communications Protection Standard

Purpose

The System and Communications Protection Standard provides documentation of the minimum technical and behavioral requirements to achieve compliance with the System and Communications Protection 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 3-1 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. 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:

Separation of System and User Functionality (SC-2):

- Separating user functionality, including user interface services, from system management functionality. System management functionality includes functions that are necessary to administer databases, network components, workstations, or servers.

Information in Shared System Resources (SC-4):

- Preventing unauthorized and unintended information transfer via shared system resources.

Denial of Service Protection (SC-5):

- Protect against or limit the effects of denial-of-service events.

Boundary Protection (SC-7):

- Monitoring and controlling communications at the external managed interfaces to the system and at key internal managed interfaces within the system.
- Implementing subnetworks for publicly assessable system components that are physically and/or logically separated from internal Agency networks.
- Connecting to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with Agency security and privacy architecture.

Access Points (SC-7(3)):

- Limiting the number of external network connections to the system to facilitate monitoring of inbound and outbound communications traffic.

Deny By Default – Allow by Exception (SC-7(5)):

- Denying network communications traffic by default and allow network communications traffic by exception at managed interfaces. Exceptions for firewalls are approved firewall rules by appropriate Agency personnel or role.

Prevent Split Tunneling for Remote Devices (SC-7(7)):

- Preventing split tunneling for remote devices connecting to systems unless the split tunnel is securely provisioned using Agency-defined safeguards.

Route Traffic to Authenticated Proxy Services (SC-7(8)):

- Routing Agency-defined internal communications traffic to Agency-defined external networks through authenticated proxy servers at managed interfaces.

Transmission Confidentiality and Integrity (SC-8):

- Protecting the confidentiality and integrity of transmitted information.

Transmission Confidentiality and Integrity (SC-8(1)):

- Implementing cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission.

Network Disconnect (SC-10):

- Terminating the network connection associated with a communications session at the end of the session or after 15 minutes of inactivity.

Cryptographic Key Establishment and Management (SC-12):

- Agency must establish and manage cryptographic keys when cryptography is employed within information systems.

Cryptographic Protection (SC-13):

- Implementing the cryptography in accordance with applicable laws, executive orders, directives, regulations, policies, standards, or guidelines.

Collaborative Computing Devices and Applications (SC-15):

- Prohibiting remote activation of collaborative computing devices and applications.

Public Key Infrastructure Certificates (SC-17):

- Issuing public key certificates under an appropriate certificate policy or obtain public key certificates from an approved service provider.

Mobile Code (SC-18):

- Authorizing, monitoring, and controlling the use of mobile code and mobile code technologies within systems.

Session Authenticity (SC-23):

- Protecting the authenticity of communication sessions.

Protection of Information at Rest (SC-28):

- Agency defines and documents the information that requires protecting the confidentiality and integrity at rest.
    - Ensure purchases that utilize mobile code and mobile code technologies includecontract language requiring the use of secure code at purchase and throughout the lifetime of the code/technology.
    - Set information systems to prevent automatic execution of active code (SC-18).

Definitions

Active content - refers to electronic documents/code that can carry out or trigger actions automatically without an individual directly or knowingly invoking the actions. This does not include scheduled batch jobs.

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.

Mobile code technology – Examples include, Java, JavaScript, ActiveX Postscript, PDF, Shockwave movies, Flash animations and VBScript.

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.

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
1.0	10/15/18	Submitted to and approved by the IT Executive Steering Committee	Reviewer: ITESC Author: DOA/DET	10/15/18
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
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:

Alan Greenberg, CISO

DocuSigned by:
Alan Greenberg
7062227F849B429

7/8/2022 | 1:55 PM CDT

Print/Type
Title

Signature

Date