260 – System and Information Integrity Standard

Purpose

The System and Information Integrity standard provides documentation of the requirements to achieve compliance with the System and Information Integrity 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:

Flaw Remediation (SI-2):

- Identifying, reporting, and correcting system flaws.
- Testing software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
- Installing security-relevant software and firmware updates within Agency-defined time periods of the release of the updates.
- Incorporating flaw remediation into the organizational configuration management process.
- Communication plans must be developed and utilized when there is a need to implement routine and/or critical or off-schedule patches.
- Executive branch agencies are responsible for systems and/or software that no longer have security patches available or have business needs that conflict with patching requirements. These systems and/or software are required to follow the DOA/DET Exception Process.

Malicious Code Protection (SI-3):

- Implementing malicious code protection mechanisms at system entry and exit points to detect

and eradicate malicious code.
- Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.
- Configure malicious code protection mechanisms to:
    - Perform periodic scans of the system based on the Agency-defined frequency, and real-time scans of files from external sources at endpoint and network entry and exit points, as the files are downloaded, opened, or executed.
    - Blocking malicious code, quarantining malicious code, or take Agency-defined actions, and send alerts to Agency-defined personnel or roles in response to malicious code detection.
    - Addressing the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

System Monitoring (SI-4):

- Monitoring the system to detect:
    - Attacks and indicators of potential attacks.
    - Unauthorized local, network, and remote connections.
- Identifying unauthorized use of the system.
- Invoking internal monitoring capabilities or deploying monitoring devices:
    - Strategically within the system to collect Agency-determined essential information.
    - At ad hoc locations within the system to track specific types of transactions of interest to the Agency.
- Analyzing detected events and anomalies.
- Adjusting the level of system monitoring activity when there is a change in the risk to Agency operations and assets, individuals, other organizations, or the Nation.
- Obtain legal opinion on regarding system monitoring activities.
- Providing Agency monitoring information to assigned personnel or roles as needed or by an Agency-defined frequency.

Automated Tools and Mechanisms for Real-Time Analysis (SI-4(2)):

- Employ automated tools and mechanisms to support near real-time analysis of events.

Inbound and Outbound Communications Traffic (SI-4(4)):

- Monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.

System Generated Alerts (SI-4(5)):

- Alert Agency-defined personnel or roles when the system generates indications of compromise or potential compromise occurs.

Wireless Intrusion Detection (SI-4(14)):

- Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

Security Alerts, Advisories, and Directives (SI-5):

- Receiving system security alerts, advisories, and directives on an ongoing basis.

- Generating internal security alerts, advisories, and directives as deemed necessary.
- Disseminating security alerts, advisories, and directives to Agency-defined personnel or roles.
- Implementing security directives in accordance with established time frames. For Federal requirements, it may require the Agency to notify the issuing organization of the degree of noncompliance.

Spam Protection (SI-8):

- Employing spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages.
- Update spam protection mechanisms when new releases are available, in accordance with Agency configuration management policy and procedures.

Information Management and Retention (SI-12):

- All State IT systems and system environments must handle and retain both information within and output from the information system(s) in accordance with the State of Wisconsin Records Retention and Disposal Policy and applicable compliance regulations

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.

DET/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 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