STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION
Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2023

170 - Incident Response Standard

Purpose

The Incident Response Standard defines an information security incident(s) for 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 3-8 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 is divided into two sections of controls. **Section One** includes the minimum baseline controls that Executive Branch agencies are to adhere to. **Section Two** includes additional controls for agencies that are subject to regulatory requirements. The list in Section Two is not all-inclusive. Agencies may have additional controls they must adhere to that are not listed here.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (IR-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - An incident response 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 incident response policy and

the associated incident response controls;

- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the incident response policy and procedures; and
- Review and update the current incident response:
    - Policy on an agency-defined frequency; and
    - Procedures on an agency-defined frequency.

Incident Response Training (IR-2):

- Provide incident response training to system users consistent with assigned roles and responsibilities:
    - Within an agency-defined time period of assuming an incident response role or responsibility or acquiring system access;
    - When required by system changes or reporting changes; and
    - Annually thereafter; and
- Review and update the incident response training content based on agency requirements and following an agency-defined event.

Incident Response Training | Breach (IR-2(3)):

- Provide incident response training on how to identify and respond to a breach, including the agency's process for reporting a breach.

Incident Response Testing (IR-3):

- Test the effectiveness of the incident response capability to identify potential weaknesses or deficiencies annually. A test can include various techniques, such as walkthroughs, tabletop exercises, simulations, and checklists.

Incident Response Testing | Coordination with Related Plans (IR-3(2)):

- Coordinate incident response testing with agency elements responsible for related plans.

Incident Handling (IR-4):

- Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection, and analysis, containment, eradication, and recovery;
- Coordinate incident handling activities with contingency planning activities;
- Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and
- Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the agency.

Incident Handling | Automated Incident Handling Processes (IR-4(1)):

- Support the incident handling process using automated mechanisms.

Incident Monitoring (IR-5):

- Track and document incidents.

Incident Reporting (IR-6):

- Require personnel to report suspected security, privacy, and supply chain incidents to the appropriate channels or personnel within an agency-defined time period.

Incident Reporting | Automated Reporting (IR-6(1)):

  - Report incidents using automated mechanisms.

Incident Reporting | Supply Chain Coordination (IR-6(3)):

  - Provide incident information to the provider of the product or service and other agencies involved in the supply chain or supply chain governance for systems or system components related to the incident.

Incident Response Assistance (IR-7):

- Provide an incident response support resource, integral to the agency incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.

Incident Response Assistance | Automation Support for Availability of Information and Support (IR-7(1)):

  - Increase the availability of incident response information and support using automated mechanisms.

Incident Response Plan (IR-8):

- Develop an incident response plan that:
  - Provides the agency with a roadmap for implementing its incident response capability;
  - Describes the structure and organization of the incident response capability;
  - Provides a high-level approach for how the incident response capability fits into the agency;
  - Meets the unique requirements for the agency, which relate to mission, size, structure, and functions;
  - Defines reportable incidents;
  - Provides metrics for measuring the incident response capability within the organization;
  - Defines the resource and management support needed to effectively maintain and mature an incident response capability;
  - Addresses the sharing of incident information;
  - Is reviewed and approved by designated agency personnel or roles on an annual basis; and
  - Explicitly designates responsibility for incident response to agency-defined entities, personnel, or roles.
- Distribute copies of the incident response plan to appropriate personnel;
- Update the incident response plan to address system and agency changes or problems encountered during plan implementation, execution, or testing;

- Communicate incident response plan changes to appropriate personnel; and
- Protect the incident response plan from unauthorized disclosure and modifications.

Incident Response Plan | Breaches (IR-8(1)):

  - Include the following in the Incident Response Plan for breaches involving personally identifiable information:
    - A process to determine if notice to individuals or other organizations, including oversight organizations, is needed:
    - An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
    - Identification of applicable privacy requirements.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies must adhere to the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may 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.

Incident Reporting | Vulnerabilities Related to Incidents (IR-6(2)):

  - Report system vulnerabilities associated with reported incidents to the appropriate agency personnel or roles.

Incident Response Assistance | Coordination with External Providers (IR-7(2)):

  - Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and
  - Identify agency incident response team members to the external providers.

Information Spillage Response (IR-9):

- Respond to information spills by:
  - Assigning designated incident response agency personnel with responsibility for responding to information spills;
  - Identifying the specific information involved in the system contamination;
  - Alerting designated agency officials of the information spill using a method of communication not associated with the spill;
  - Isolating the contaminated system or system component;
  - Eradicating the information from the contaminated system or component;
  - Identifying other systems or system components that may have been subsequently contaminated; and
  - Performing additional actions as required by the agency.

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 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	10/29/19	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

A11B57ECEC77402...

8/1/2023 | 1:49 PM CDT

Print/Type
Title

Signature

Date