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 3-1 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:

Incident Response Training (IR-2):

- Providing 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.
- Reviewing and updating the incident response training content based on agency requirements and following an Agency-defined event.

Incident Response Testing (IR-3):

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

- If applicable, Executive Branch Agencies shall test the effectiveness of their incident response capabilities to identify potential weaknesses or deficiencies annually. A test can include various techniques, such as walkthroughs, tabletop exercises, simulations, and checklists.

Incident Handling (IR-4):

- Implements an incident handling capability for security and privacy incidents that includes preparation, detection, and analysis, containment, eradication, and recovery.
- Coordinates incident handling activities with contingency planning activities.
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implementing the resulting changes accordingly.
- Ensures the rigor, intensity, scope, and results of incident handling activities are comparable and predictable in the Agency.

Incident Monitoring (IR-5):

- Tracking and documenting incidents.

Incident Reporting (IR-6):

- Agencies are to require personnel to report suspected security, privacy, and supply chain incidents through the appropriate channels or personnel within the agencies within three days of the suspected 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 Plan (IR-8):

- Developing an incident response plan that:
    - Provides the agency with 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 Agency-defined personnel or roles on an annual basis.
    - Explicitly designates responsibility for incident response to Agency-defined entities, personnel, or roles.
- Distributing copies of the incident response plan to appropriate personnel.
- Updating the incident response plan to address system and agency changes or problems

encountered during plan implementation, execution, or testing.
- Communicating incident response plan changes to appropriate personnel.
- Protecting the incident response plan from unauthorized disclosure and modifications.

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 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