150 – Contingency Planning Standard

Purpose

The purpose of the Contingency Planning Standard is to is to set forth requirements and expectations related to and supporting a resilient posture against unscheduled interruptions/downtime to the State of Wisconsin information systems and data, and to ensure that its staff and business partners are well-informed of their responsibilities when a disruption of business operations occurs and requires immediate action. Additionally, this standard provides requirements for the development of a contingency plan to restore an established level of service to State IT systems, system environments, and services as required by the Contingency Planning Policy and the Incident Response Policy.

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

Policy and Procedures (CP-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A contingency planning policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.

    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the contingency planning policy and procedures.
- Review and update the current contingency planning:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Contingency Plan (CP-2):

- Develop a contingency plan for the system that:
  - Identifies essential mission and business functions and associated contingency requirements.
  - Provides recovery objectives, restoration priorities, and metrics.
  - Addresses contingency roles, responsibilities, assigned individuals with contact information.
  - Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure.
  - Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented.
  - Addresses the sharing of contingency information.
  - Is reviewed and approved by designated agency personnel.
- Distribute copies of the contingency plan to key contingency personnel (identified by name and/or by role) and organizational elements.
- Coordinate contingency planning activities with incident handling activities.
- Review the contingency plan for the system annually.
- Update the contingency plan to address changes to the agency, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.
- Communicate contingency plan changes to key contingency personnel (identified by name and/or by role) and organizational elements.
- Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training.
- Protect the contingency plan from unauthorized disclosure and modification.

Contingency Plan | Coordinate with Related Plans (CP-2(1)):

- Coordinate contingency plan development with organizational elements responsible for related plans.

Contingency Plan | Resume Mission and Business Functions (CP-2(3)):

- Plan for the resumption of all or essential mission and business functions within a defined time period of contingency plan activation.

Contingency Plan | Identify Critical Assets (CP-2(8)):

- Identify critical system assets supporting all or essential mission and business functions.

Contingency Training (CP-3):

- Provide contingency training to system users consistent with assigned roles and responsibilities:
  - Prior to assuming a contingency role or responsibility.
  - When required by system changes.
  - Annually thereafter.
- Review and update contingency training content annually and following agency-defined events (i.e., contingency plan testing, an actual contingency, assessment or audit findings, security or privacy incidents, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines).

Contingency Plan Testing (CP-4):

- Test the contingency plan for the system annually using tests (i.e., checklists, walk-through and tabletop exercises, simulations, comprehensive exercises) to determine the effectiveness of the plan and the readiness to execute the plan.
- Review the contingency plan test results.
- Initiate corrective actions, if needed.

Contingency Plan Testing | Coordinate with Related Plans (CP-4(1)):

- Coordinate contingency plan testing with organizational elements responsible for related plans.

Alternate Storage Site (CP-6):

- Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information.
- Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Alternate Storage Site | Separation from Primary Site (CP-6(1)):

- Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Alternate Storage Site | Accessibility (CP-6(3)):

- Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Alternate Processing Site (CP-7):

- Establish an alternate processing site, including necessary agreements to permit the transfer and

resumption of system operations for essential mission and business functions, within a time period consistent with recovery time and recovery point objectives, when the primary processing capabilities are unavailable.

- Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within an agency-defined time period for transfer and resumption.
- Provide controls at the alternate processing site that are equivalent to those at the primary site.

Alternate Processing Site | Separation from Primary Site (CP-7(1)):

- Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Alternate Processing Site | Accessibility (CP-7(2)):

- Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Alternate Processing Site | Priority of Service (CP-7(3)):

- Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Telecommunications Services (CP-8):

- Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within an agency-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Telecommunications Services | Priority of Service Provisions (CP-8(1)):

- Develop primary and alternate telecommunications service agreements that contain priority-or-service provisions in accordance with availability requirements (including recovery time objectives).

Telecommunications Services | Single Points of Failure (CP-8(2)):

- Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

System Backup (CP-9):

- Conduct backups of user-level information contained in system components on an agency-defined frequency consistent with recovery time and recovery point objectives.
- Conduct backups of system-level information contained in the system on an agency-defined frequency consistent with recovery time and recovery point objectives.
- Conduct backups of system documentation, including security- and privacy-related documentation on an agency-defined frequency consistent with recovery time and recovery point objectives.
- Protect the confidentiality, integrity, and availability of backup information.

System Backup | Testing for Reliability and Integrity (CP-9(1)):

- Test backup information on an agency-defined frequency to verify media reliability and information integrity.

System Backup | Cryptographic Protection (CP-9(8)):

- Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information.

System Recovery and Reconstitution (CP-10):

- Provide for the recovery and reconstitution of the system to a known state, within an agency-defined time period consistent with recovery time and recovery point objectives, after a disruption, compromise, or failure.

System Recovery and Reconstitution | Transaction Recovery (CP-10(2)):

- Implement transaction recovery for systems that are transaction-based.

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.

Contingency Plan | Capacity Planning (CP-2(2)):

- Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

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.

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.

Summary of Solution (SOS) - A "postmortem" analysis of an outage (or major incident) which affects two

or more Agencies to be shared with appropriate Executive Branch Agency partners.

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	07/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	07/31/23
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
DEEB606FC2524A8...

7/31/2024 | 4:05 PM CDT

Print/Type | Signature | Date

Title