150 – Contingency Planning Standard

Purpose

The Contingency Planning Standard provides documentation of the 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

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:

Contingency Plan (CP-2):

- Developing 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; and
  - Is reviewed and approved by Agency-approved personnel;
- Distributing copies of the contingency plan to key contingency personnel (identified by name and/or by role) and organizational elements;

- Coordinating contingency planning activities with incident handling activities;
- Reviewing the contingency plan for the system annually;
- Updating the contingency plan to address changes to the agency, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
- Communicating contingency plan changes to key contingency personnel (identified by name and/or by role) and organizational elements;
- Incorporating lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
- Protecting the contingency plan from unauthorized disclosure and modification.

Coordinate with Related Plans (CP-2(1)):

- Coordinating contingency plan development with organization elements responsible for related plans.

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

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

Identify Critical Assets (CP-2(8)):

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

Contingency Training (CP-3):

- Providing contingency training to system users consistent with assigned roles and responsibilities:
  - Prior to assuming a contingency role or responsibility;
  - When required by system changes; and
  - Annually thereafter; and
- Reviewing and updating 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):

- Testing 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;
- Reviewing the contingency plan test results; and
- Initiating corrective actions, if needed.

Alternate Storage Site (CP-6):

- Establishing an alternate storage site, including necessary agreements to permit the storage and

retrieval of system backup information; and

- Ensuring that the alternate storage site provides controls equivalent to that of the primary site.

Separation from Primary Site (CP-6(1)):

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

Accessibility (CP-6(3)):

- Identifying 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):

- Establishing 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.
- Making 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; and
- Providing controls at the alternate processing site that are equivalent to those at the primary site.

Separation from Primary Site (CP-7(1)):

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

Accessibility (CP-7(2)):

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

Priority of Service (CP-7(3)):

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

Telecommunications Services (CP-8):

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

Priority of Service Provisions (CP-8(1)):

- Developing primary and alternate telecommunications service agreements that contain

priority-or-service provisions in accordance with availability requirements (including recovery time objectives).

Single Points of Failure (CP-8(2)):

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

System Backup (CP-9):

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

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

- Testing backup information on an Agency-defined frequency to verify media reliability and information integrity.

Cryptographic Protection (CP-9(8)):

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

System Recovery and Reconstitution (CP-10):

- Providing 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.

Transaction Recovery (CP-10(2)):

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

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.

Summary of Solution (SOS) - A "post mortem" 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 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