Information Technology Disaster Recovery Planning Standard

From the Office of the Chief Information Officer, State of Minnesota

Version: 1.8
Effective Date: 1/1/2016
Revised: 12/31/2024
Approved: John Israel, State Chief Information Security Officer **Date:** 3/20/2025

Standard Statement

Information technology disaster recovery plans must be in place that align with the priorities and recovery timelines of state agency critical priority services to ensure the State of Minnesota is adequately managing the risk of system and service interruptions.

Employees must abide by the terms of this standard. Employees who violate this standard may be subject to discipline, up to and including discharge.

Table 1. Disaster Recovery Planning Controls

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization

1	Information Technology Disaster Recovery (IT DR) Plan	An IT DR plan must be developed and maintained for critical systems. Critical systems support state agency critical priority services (priority 1 and 2 services) as defined in agency business impact analyses (BIA). Plans must:
		• Include the following information gathered from business priority service owners to develop recovery strategies:
		  ○ Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and restoration priorities.
		  ○ Impacts to the priority service and its customers if the system is disrupted, compromised, or fails.
		  ○ System users and their primary and alternate work locations.
		  ○ Key processing times during the week, month, or year when system availability is especially important.
		  ○ Essential records stored or created by the system.
		• Identifies information system assets supporting state critical priority services.
		• Documents roles, responsibilities, and assigned individuals.
		• Addresses eventual, full system restoration, without deterioration of the security measures originally planned and implemented.
		• Documents user-level information, system-level information, and security-related documentation backup frequency.
		• Aligns with IT incident management and continuity of operations incident response activities.
		The plan must be reviewed and approved by IT leadership in conjunction with business owners.
		Some data contained in an IT disaster recovery plan is “security information” within the meaning of Minnesota Statutes, Section 13.37, and private data within the meanings of Minnesota Statutes, Sections 13.356 and 13.43. The plan must be protected from unauthorized disclosure and modification.
			Moderate
			High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
2	IT DR Plan Distribution	Distribute copies of the IT DR plan to personnel with a need to know, including MNIT, state agency leaders, and key vendors.	Moderate High
3	IT DR Plan Review	Review and update the IT DR plan: • To address system or organizational changes. • To address problems encountered during plan implementation or execution. • To address test results and identified gaps. • At least annually. Communicate IT DR plan changes to personnel with a need to know.	Moderate High
4	IT DR Plan and Procedures Training	Personnel must obtain IT DR plan and procedures training consistent with their assigned roles and responsibility: • Within ninety (90) days of assuming an IT DR plan role or responsibility. • Following significant system or recovery strategy changes. • Following IT DR plan updates. • At least annually.	Moderate High
5	IT DR Plan Testing	The IT DR plans for systems supporting state critical priority services must be tested at least annually to determine the effectiveness of the plan and MNIT's readiness to execute the plan. IT DR plan testing must be coordinated with state agency partners responsible for related plans. Test results must be documented in an after-action report and improvement plan (AAR/IP) and identified gaps addressed.	Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
6	Capacity Planning	Planning must be conducted to ensure the necessary capacity for information processing, telecommunications, and utility and other support services are available to recover critical systems following an interruption, emergency, or disaster. .	Moderate High
7	Alternate Storage Site	An alternate storage site must be established for systems supporting state critical priority services, including necessary agreements to permit the storage and recovery of system backup information. The alternate storage site must: • Be separated from the primary storage site to reduce susceptibility to the same threats as identified in a risk assessment. • Provide required information security safeguards. • Comply with all applicable state and federal requirements. Identify and document multiple travel routes to local and regional sites in the event IT professionals must report to the site because of an area-wide emergency or disaster.	Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
8	Alternate Processing Site	Establish an alternate processing site including necessary agreements to permit the resumption of system operations for critical priority services within applicable recovery time objectives when the primary processing capabilities are unavailable. Ensure that equipment and supplies required to resume operations are available at the alternate site, or contracts are in place to support delivery to the site in time to support the resumption. Ensure the alternate processing site is separated from the primary processing site to reduce susceptibility to the same threats as identified in a risk assessment. Provides required information security safeguards. Identify multiple travel routes to local and regional alternate processing sites in the event IT professionals must report to a site because of an area-wide emergency or disaster	Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
9	Telecommunications Services	Establish alternate telecommunications services when redundant telecommunication services are not available from Minnesota IT Services. Where necessary, agreements must be established to permit the resumption of system operations for critical priority services within the recovery time objective specified when the primary telecommunications capabilities are unavailable. If agreements with alternate telecommunications providers are needed, they must: • Ensure alternate telecommunications agreements are in place to permit resumption of the system within agreed upon Recovery Time Objectives (RTO). • Contain priority-of-service provisions in accordance with state agency availability requirements, including recovery time objectives. • Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.	Moderate High
10	System Backup	Conduct backups of user-level information, system-level information, and security-related documentation consistent with the defined frequency in the IT DR plan. Critical systems must have three generations of backups (full as well as all related incremental or differential backups) stored off site. Protect the confidentiality, integrity, and availability of backup information at storage sites. Off-site and on-site backups must be logged with name, date, time, and action.	Moderate High
11	Testing for Reliability/Integrity	Test backup information at least annually to verify media reliability and information integrity.	Moderate High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
12	Transaction Recovery	Transaction recovery must be implemented for transaction-based systems.	Moderate High
13	System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state after a disruption, compromise, or failure in a trusted, secure, and verifiable manner. Secure information system recovery and reconstitution includes, but is not limited to: • Reset of all system parameters (either default or MNIT established). • Reinstallation of patches. • Reestablishment of configuration settings. • Reinstallation of application and system software. • Full testing of the system.	Moderate High

Reason for the Standard

Interruptions to information technology systems can have a severe impact on the State of Minnesota's ability to provide critical priority services. IT DR plans provide a roadmap to recover systems so they are available to support the continuation of State critical priority services in the event of an emergency or system disruption with minimal downtime, data loss and impact to State operations.

Roles & Responsibilities

- Employees, Vendors, and Contractors
    - Be aware of and follow relevant continuity of operations, IT DR and information security policies, standards, and procedures.
    - Ensure continuity of operations, IT DR and information security is incorporated into processes and procedures.
    - Ensure vendors and contractors are following required continuity of operations, IT DR and information security controls and have the required continuity of operations and IT DR plans and capabilities.
    - Contact the MNIT continuity of operations coordinator, information security staff or email GRC@state.mn.us with questions about the information security, continuity of operations and IT DR policies, standards, or procedures.
- Supervisors and Managers

    - Ensure employees and contractors are proficient in the continuity of operations, IT DR and information security policies, standards and procedures that are relevant to their role.
    - Hold employees accountable for following the continuity of operations, IT DR and information security policies, standards, and procedures.
- Information Technology Personnel
    - Apply appropriate controls to the design, operation and maintenance of systems, processes, and procedures in conformance with the continuity of operations, IT DR and information security policies, standards, and procedures.
- Information Security Personnel
    - Develop, maintain, and assess compliance with the information security policies, standards, and procedures.
    - Develop, maintain, and implement a comprehensive information security program.
    - Provide training on information security policies, standards, and procedures.
    - Assist agencies and personnel with understanding and implementing information security policies, standards, and procedures.
- Agency Data Practices Personnel
    - Assist agencies and personnel with questions on proper data use, collection, storage, destruction, and disclosure.
- MNIT Continuity of Operations Coordinator
    - Develop, maintain, and assess MNIT compliance with the continuity of operations and IT DR policies, standards, and procedures.
    - Develop, maintain, and implement a comprehensive MNIT continuity of operations program.
    - Provide training on continuity of operations and IT DR policies, standards, and procedures to MNIT employees.
    - Assist agencies and personnel with understanding and implementing continuity of operations and IT DR policies, standards, and procedures.

Applicability

This standard applies to all departments, agencies, offices, councils, boards, commissions, and other entities in the executive branch of Minnesota State Government.

Related Information

Information Technology Disaster Recovery Planning Policy

Governor's Executive Order 19-22

Governor's Executive Order 19-23

State Standards and Authoritative Source Cross Mapping

Glossary of Information Security Terms

History

Table 2. Version History

Version	Description	Date
1.0	Initial Release	7/8/2015
1.1	Added Compliance Enforcement Date	12/29/2015
1.2	Updated Compliance Enforcement Date and New Template	12/20/2016
1.3	Updated Compliance Enforcement Date and New Template	10/26/2017
1.4	New document title. Updated to better align with NIST. Updated referenced Governor's executive orders.	3/10/2020
1.5	Scheduled Document Refresh	11/1/2021
1.6	Scheduled document refresh	10/1/2022
1.7	Added clarified wording from COOP team; version number and revision date update	10/1/2023
1.8	Added enforcement language; updated version and revision date	12/2/2024

Contact

GRC@state.mn.us