

SEC 12

State CIO Adopted: November 16, 2023

TSB Approved: November 28, 2023

Sunset Review: November 28, 2026



Washington Technology Solutions

Replaces:

Document IT Policy 151

December 6, 2016

INFORMATION TECHNOLOGY DISASTER RECOVERY PLANNING POLICY

See Also:

RCW [43.105.054](#) OCIO Governance

RCW [43.105.205](#) (3) Higher Ed

RCW [43.105.020](#) (22) "State agency"

RCW [43.105.450](#) OCS Governance

[Asset Management Policy](#)

[Backup and Recovery](#)

[Security Awareness Training Policy](#)

[Directive 13-02 Continuity of Operations](#)

- 1. Agencies must develop Information Technology (IT) Disaster Recovery (DR) plan(s) in support of the agency [Continuity of Operations Plan \(COOP\)](#), including [services](#), and applications reported as [mission critical and business essential](#).**
 - a. DR plan(s) are required for each technology necessary to support and deliver the agency's essential functions documented in the agency's COOP.
 - b. DR plan(s) must include, document, and account for interdependencies with:
 - i. Roles critical for executing the plan(s).
 - ii. Other [systems](#).
 - iii. Internal or externally hosted applications.
 - iv. Inter-agency service providers, such as WaTech, DES, or OFM.
 - v. External parties such as public cloud providers, Software as a Service ([SaaS solutions](#)), and data storage.
 - c. DR plan(s) must be reviewed, updated, and exercised at least every other year.
 - i. Within 90 days of the production date, agencies must review, update, and exercise plans for new applications or services or those that undergo significant changes or major upgrades.
 - ii. Agencies must document objectives of the exercise.
 - iii. Agencies must document exercise results.
 - iv. Agencies must identify and document corrective actions and/or risk mitigations based on exercise results and update the DR plan accordingly.

- v. Agencies must demonstrate in their documentation that service providers or other external parties that support critical services or essential functions comply with annual exercise requirements.
2. **Agencies must ensure employees, contractors, and external parties are engaged in exercises and/or complete training as to their role in executing the agency's DR Plan(s).** [See the Security Awareness and Training Policy.](#)
3. **Agency heads are responsible for ensuring compliance with this policy and must approve the annual DR plan(s).**

REFERENCES

1. [Definition of Terms Used in WaTech Policies and Reports.](#)
2. [NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems](#)
3. [Disaster Recovery/Business Guidelines \(wa.gov\)](#)
4. NIST Cybersecurity Framework Mapping
 - Protect. Information Protection Processes and Procedures - 9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
 - Protect. Information Protection Processes and Procedures – 10: Response and recovery plans are tested.
 - Respond. Communications - 1: Personnel know their roles and order of operations when a response is needed.
 - Respond. Communications – 3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.
 - Respond. Communications – 4: Coordination with stakeholders occurs consistent with response plans.
 - Respond. Response Planning -1: Response plan is executed during or after an incident.
 - Recover. Recovery Planning -1: Recovery plan is executed during or after a cybersecurity incident.

CONTACT INFORMATION

- For questions about this policy, please email the [WaTech Policy Mailbox](#).
- For technical assistance, please email [WaTech Disaster Recovery Mailbox](#).