SEC-12
State CIO Adopted: November 16, 2023
TSB Approved: November 28, 2023
Sunset Review: November 28, 2026

WaTech
Washington Technology Solutions

Replaces:
IT Policy 151
Disaster Recovery Planning
December 6, 2016

INFORMATION TECHNOLOGY

DISASTER RECOVERY PLANNING POLICY

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
RCW 43.105.020 (22) "State agency"
RCW 43.105.450 OCS Governance
SEC-04 Asset Management Policy
SEC-04-01-S Data Backup and Recovery Standard
Directive 13-02 Continuity of Operations Preparation

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, the Department of Enterprise Services, or the Office of Financial Management.

        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 SEC-03 IT Security and Privacy Awareness 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. SEC-03 IT Security and Privacy Awareness Training Policy.
3. NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.
4. NIST Cybersecurity Framework Mapping 2.0:
   - ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.
   - ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.
   - PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.
   - RS.CO-03: Information is shared with designated internal and external stakeholders.
   - RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.
   - RS.MA-04: Incidents are escalated or elevated as needed.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For technical questions, please email the Enterprise Risk Management Mailbox.