SEC-04-01-S
State CIO Adopted: June 8, 2023
TSB Approved: June 8, 2023
Sunset Review: June 8, 2026

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (8.4)
December 11, 2017

DATA BACKUP AND RECOVERY STANDARD

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 Office of Cybersecurity
NIST 800-209 Security Guideline for Storage Infrastructure

1. **Each agency must establish backup and recovery procedures for data processed and stored on IT resources.**

    a. Agencies are responsible for ensuring the backup of their data. Agencies must ensure the following resources have immutable backups:

        i. Mission critical.

        ii. Business essential.

        iii. Containing category 3 or category 4 data as defined in the SEC-08-01-S Data Classification Standard.

    b. Agencies must determine backup rotation requirements on the results of a business impact analysis and IT risk assessment.

    c. Agencies that use backup media must establish a backup rotation strategy based on the following factors:

        i. Useful life of the backup media.

        ii. The system's Recovery Point Objective (RPO)

        iii. The volume of data required to complete a single backup.

2. **Agencies using a vendor service to perform their backups are responsible for coordinating with the vendor to document the backup plan and ensuring that:**

    a. Backups are completed successfully.

    b. Backup and recovery plan, procedures, and retention schedules are

documented.

c. Agency management or their designee must review monthly and ensure that appropriate, proper backups are being made.

d. Backup frequency must be based on the criticality and sensitivity of the data along with the Recovery Time Objective (RTO).

e. At least two copies of the backups must be maintained to ensure recovery should any of the backups not recover properly, with at least one of those backups stored off-site according to Cybersecurity & Infrastructure Security Agency (CISA) Data Backup Options and best practices:

   i. Maintain three (3) copies of backups: one (1) primary and two (2) redundant copies.

   ii. Maintain the backups on different storage media.

   iii. Store one (1) copy offsite.

f. Backup logs, backup reports, or other backup audit trails must be maintained to track backup media; the information, data, or files backed up on the media, the date and time of the backup, and the successful completion of the backup.

g. Agencies and host IT service providers must specify responsibilities and a schedule for backups in a written agreement as per the Data Sharing Policy.

3. **Agencies performing their own backups must document the data backup plan for the IT systems in their environments including:**

a. The business criticality of resources processing agency data. See the MGMT-01-01-S Technology Portfolio Foundation – Applications Standard for additional information.

b. Identification of the system, application, or data to be recovered. Agency recovery plans must prioritize business essential and mission critical systems.

c. Network and system architecture diagrams, system setup documentation, and any other information required for full recovery of systems, applications, or data.

d. Identification and contact information of the primary and secondary staff responsible for accomplishing the recovery.

e. Location of backups.

f. Specific step-by-step instructions for accomplishing the recovery.

g. Any additional requirements resulting from following SEC-12 IT Disaster Recovery Planning policy.

4. **Agencies must revise the recovery strategies upon the addition of computing and network devices to their environments.**

5. **Agencies must perform and document testing of their data backup and recovery plan.**
    a. Agencies must develop, document, and follow their procedures to test their backup and recovery plan at least annually.

    b. Agencies must document results from each area (system, application, and data) of the backup and recovery tests, including the following:

        i. Success or failure of the backup or recovery test.

        ii. Identification of the failure root cause(s).

        iii. Timeline for remediation of the root cause(s).

6. **Agencies must maintain at least one copy of the recovery procedure off-site and revise the backup procedure at least annually.**

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports
2. SEC-08-01-S Data Classification Standard
3. Washington Secretary of State Retention Schedules
4. MGMT-01-01-S Technology Portfolio Foundation Standard- Applications
5. SEC-12 Information Technology Disaster Recovery Planning
6. SEC-08 Data Sharing Policy
7. CISA Data Backup Options
8. NIST Cybersecurity Framework Mapping:

    - Protect.Information Protection Processes and Procedures-4 (PR.IP-4): Backups of information are conducted, maintained, and tested
    - Protect.Data Security-4 (PR.DS-4): Adequate capacity to ensure availability is maintained.

- Recover.Recovery Planning-1 (RC.RP-1): Recovery plan is executed during or after a cybersecurity incident.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.