Policy & Standard Background

Name: Data Backup and Recovery Standard

Replaces IT Security Standard 141.10 (8.4)

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability. This standard draws from NIST 800-209 - Security Guideline for Storage Infrastructure. This provides agencies with a single document with data backup and recovery requirements applicable across various contexts.

What is the business case for the policy/standard?

- This standard helps agencies safeguard and prioritize the data they store or entrust to vendors.
- This standard helps agencies document and test their backup and recovery activities.

What are the key objectives of the policy/standard?

The objectives of this standard are:

- To ensure agencies are prepared for planned or unplanned interruptions of service.
- To reduce the impact of service interruptions to the agency's customers.

How does policy/standard promote or support alignment with strategies?

Strategic Planning | Washington Technology Solutions

This standard helps agencies ensure the recovery of vital resources in the event of failure or loss of data. This supports a security and privacy for a safe community and effective government.

What are the implementation considerations?

- Agencies will need resources to create, revise, document and test plans.
- Agencies will need to ensure contracts meet data backup and recovery standards.

How will we know if the policy is successful?

- Agencies will document successful testing of backup and recovery plans.
- Agencies will validate that vendors are meeting contract requirements on a monthly basis.

State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10
Section 8.4
December 11, 2017

DATA BACKUP AND RECOVERY STANDARD

See Also:
RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) State Agency
RCW 43.105.450 (7c) IT Security

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 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 monthly review 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). See the Technology Portfolio Foundation – Applications Standard 112.10 for additional information.

    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 CISA 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 IT Standard 112.10 - Technology Portfolio Foundation – Applications 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 to accomplish the recovery.

    e. Location of backups.

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

    g. Any additional requirements resulting from following 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. NIST 800-209 - Security Guideline for Storage Infrastructure

2. Definition of Terms Used in WaTech Policies and Reports
3. Technology Portfolio Foundation Standard- Applications
4. Information Technology Disaster Recovery Planning
5. Data Sharing Policy
6. Data Classification Standard
7. Washington Secretary of State Retention Schedules
8. CISA Data Backup Options
9. 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 contact the WaTech Policy Mailbox.
- To request a Security Design Review, please contact the Security Design Review Mailbox.