WaTech
Washington Technology Solutions

Disaster Recovery Planning Policy Background

New, Update or Sunset Review? Sunset Review.

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.

This is an update to the existing policy 151. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability. Updates to this standard draw from NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

What is the business case for the policy/standard?

- Disaster recovery planning is essential for ensuring that mission critical and business essential functions can be resumed in the event of a disruption.
- Implementation of governance that limits runaway liability to operational, financial, safety, and reputational impacts

What are the key objectives of the policy/standard?

- Create a common understanding of disaster recovery planning requirements.
- Require testing of disaster recovery plans to validate contingency and recovery procedures.

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

Disaster recovery planning strengthens IT architecture security. Documentation of planning and validation supports accountable government.

What are the implementation considerations?

- Implementing a DRBC program requires an investment in planning, resources, and regular testing

- Small agencies have the option of contracting WaTech for support. WaTech will also provide templates and consultation for DR planning for agencies of all sizes.
- Prioritization of training and testing and coordination of efforts for interdependent systems.

How will we know if the policy is successful?

Specific: All agencies will document and test disaster recovery plans for mission critical and business essential functions.
Measurable: Agencies will validate test plans.
Achievable: The requirement for exercising plans was adjusted to every other year to ensure agencies have time to exercise each component of the plan.
Relevant: The recent pandemic demonstrated the need for agility in returning to normal operations that are not always identical to the original state.
Timebound: Agencies must complete DR reviews and testing annually as a minimum.
Equitable: Agencies of any size can rely on WaTech for support with DR planning, templates and tools.

SEC 12
State CIO Adopted: Month 1 2023
TSB Approved: Month 1 2023
Sunset Review: Month 1 2023

WaTech
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 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

- Services Suggested Definition: *A service is a means of delivering **value** to customers by facilitating **outcomes** that customers want to achieve without the ownership of specific **costs** and **risks**.*
- Definition of Terms Used in WaTech Policies and Reports.
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- Disaster Recovery/Business Guidelines (wa.gov)
- 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.