Policy Name: Data Backup and Recovery
Section: 3000 Operational: 3100 Administrative
Policy Number: 0000

Purpose: This policy establishes the framework for the secure and reliable backup and recovery of digital data and systems critical to the operations of the District. It ensures continuity of services in the event of data loss due to cyberattacks, natural disasters, hardware failure, or human error.

Reference: None applicable

Policy:

Scope

This policy applies to all District staff, contractors, and volunteers who handle or manage digital data, including but not limited to administrative records, registration systems, financial data, and communications. This policy does not address compliance with Washington State records management requirements

Policy Statement

The District will maintain a robust data backup and recovery system that:

1. Protects sensitive and operational data.
2. Ensures timely recovery of services.
3. Complies with Washington State standards and public records laws.

Backup Strategy

The District will follow the 3-2-1 backup rule:

1. Maintain three copies of all critical data.
2. Store backup files on both Network Attached Storage (NAS) and cloud-based devices.
3. Keep one copy off-site or in the cloud to ensure resilience against regional disasters.

Backup Procedures

Frequency: Daily incremental backups and weekly full backups for critical systems.

Storage Locations:

1. On-site secure NAS.
2. Cloud-based storage with encryption.
3. Off-site physical storage (if applicable).

Retention: Backups will be retained for a minimum of 90 days unless otherwise required by law or operational need.

Encryption: All backup data must be encrypted both in transit and at rest.

Roles and Responsibilities

IT Manager: Oversees implementation, monitoring, and testing of backup systems.

Executive Services: Understand and oversee the archival and record keeping requirements.

Staff: Follow procedures for saving and storing data in designated systems.

Managers, Division Directors, Superintendents: Encourage, teach and remind staff of their responsibilities.

Recovery Planning

The District will maintain a Data Backup and Recovery Policy that:

1. Identifies critical systems and data loss incidents.
2. Defines recovery time objectives (RTO) and recovery point objectives (RPO).
3. Includes procedures for manual operations during outages.
4. Designates alternate work locations if primary facilities are compromised.

Testing and Validation

1. Backup systems will be tested quarterly to ensure data integrity and recoverability.
2. Failed backups must be addressed immediately.
3. Annual review of backup and recovery plans will be conducted to reflect changes in technology or operations.

Training and Awareness

New employees will be instructed on proper file storage during onboarding.

Compliance and Review

This policy will be reviewed on a regular basis and updated as needed to comply with:

1. Washington State Auditor's Office guidelines.
2. District Operational Policies.

Backup Tools and Technologies

To ensure secure and reliable employee data protection, District IT staff may utilize a combination of the following tools and platforms:

Local Backup Solutions: Microsoft Windows 0365

Cloud-Based Backup Services: Microsoft Azure Backup

Hybrid Backup Platforms: Synology Hyper Backup

All cloud-based systems containing District data must be vetted by District IT staff and provide secure server data backups.

Data Breach Response

In the event of a data breach—defined as unauthorized access, disclosure, or loss of sensitive or protected data, the District will follow a structured response protocol to minimize harm, ensure transparency, and comply with legal obligations.

1. Detection and Reporting:
    a. Immediate reporting to IT Director.
    b. Use of automated monitoring systems (OpenText Core Endpoint Protection).

2. Initial Assessment:
    a. Assess nature, scope, and type of data affected.

3. Containment and Mitigation:

a. Isolate affected systems.
b. Reset credentials and patch vulnerabilities.

4. Notification:
    a. Notify individuals and authorities per RCW 19.255.010 and federal laws.

5. Documentation and Reporting:
    a. Compile incident report and share with Executive Director to determine further action.

6. Post-Incident Review:
    a. Identify root causes and improve protocols.

7. Prevention and Training:
    a. Annual cybersecurity training and regular audits.

Data Recovery Procedures

In the event of data loss due to system failure, human error, cyberattack, or natural disaster, District IT staff will follow structured recovery procedures to restore operations efficiently and securely.

1. Recovery Objectives:
    a. RTO: Restore critical systems within 24 hours.
    b. RPO: Data loss must not exceed 48 hours.

2. Recovery Process:
    a. Incident Identification
    b. Backup Verification
    c. Restoration
    d. Validation
    e. Documentation

3. Communication:
    a. Notify directors, managers, and applicable staff.

4. Continuous Improvement:
    a. Review and update recovery procedures and conduct refresher training.