SOP: Data Backup and Disaster Recovery Routines

This SOP details the **data backup and disaster recovery routines**, encompassing scheduled data backups, secure storage solutions, verification of backup integrity, disaster recovery planning, and regular testing of recovery procedures. The goal is to ensure the continuity of business operations by protecting critical data against loss, corruption, or disasters, and enabling swift restoration in the event of system failures or data breaches.

1. Purpose

To define standardized procedures for data backup and disaster recovery that safeguard critical information and facilitate business continuity in the event of data loss or system outages.

2. Scope

This SOP applies to all digital data, systems, and infrastructure managed by the organization that contain business-critical information.

3. Responsibilities

- **IT Manager:** Oversight of backup and recovery procedures, review and update of SOP.
- **System Administrators:** Ensure execution of backup schedules, testing, and documentation.
- **All Employees:** Report any incidents of data loss or suspected corruption immediately.

4. Backup Procedures

1. **Data Identification:**
    - Identify and list critical data sources (servers, databases, endpoints).
2. **Backup Schedule:**
    - **Full backup:** Weekly (e.g., Sundays at midnight).
    - **Incremental/differential backup:** Daily between full backups.
3. **Backup Storage:**
    - Maintain at least two backup copies: onsite (secure location) and offsite (cloud or remote server).
    - Encrypt all backup data both in transit and at rest.
    - Retain backups for a minimum of 30 days or according to regulatory requirements.
4. **Backup Verification:**
    - Automatically verify backup integrity after completion.
    - Generate and review backup reports daily.

5. Disaster Recovery Procedures

1. **Incident Response:**
    - Activate the disaster recovery plan upon detection of data loss, corruption, or major system failure.
2. **Restoration Process:**
    - Identify affected systems and data.
    - Restore the latest verified backup to affected systems.
    - Confirm system functionality and data integrity post-restoration.
3. **Communication:**
    - Notify stakeholders of the incident, actions taken, and expected timeline for recovery.
    - Document all actions during disaster recovery for post-mortem analysis.

6. Testing and Review

- Conduct scheduled recovery drills at least bi-annually to test recovery procedures.
- Document test results and update procedures based on findings.
- Review and update the disaster recovery plan annually or when significant system changes occur.

7. Documentation

- Maintain records of all backups: schedules, locations, verification logs, and drills.

- Keep disaster recovery documentation accessible and up-to-date for all relevant personnel.

8. References

- Organizational Information Security Policy
- Regulatory Data Retention Guidelines
- Disaster Recovery Plan Template

9. Revision History

Version	Date	Description	Author
1.0	2024-06-18	Initial Template Creation	IT Manager