# SOP: Backup and Data Storage Procedures

This SOP defines **backup and data storage procedures** to ensure the security, integrity, and availability of critical data. It covers protocols for regular data backups, selection of appropriate storage media, data encryption and access controls, retention schedules, verification and testing of backup copies, and disaster recovery planning. The purpose is to minimize data loss risks and maintain business continuity through systematic and reliable data management practices.

## 1. Purpose

To establish standardized procedures for backing up and storing organizational data, ensuring its security, integrity, and availability.

## 2. Scope

This procedure applies to all electronic data generated, processed, or stored by [Organization Name].

## 3. Responsibilities

- **IT Department:** Executes and monitors backup operations, maintains backup systems, and manages restore procedures.
- **Data Owners:** Ensure data is stored in designated locations for backup coverage.
- **Management:** Reviews and approves backup strategies and schedules.

## 4. Definitions

- **Backup:** A copy of data made to restore the original in case of data loss.
- **Storage Media:** Physical or cloud-based devices used for storing backup data.
- **Retention Schedule:** The defined period for which backup data will be preserved.
- **Encryption:** Protecting data by converting it into a coded format.

## 5. Procedure

1. **Backup Schedule**
    - Critical systems: Daily incremental + weekly full backups.
    - User data: Nightly differential backups.
    - Schedule automated backups outside peak business hours.
2. **Selection of Storage Media**
    - Utilize secure cloud services and/or encrypted external drives/tapes.
    - Store at least one backup copy offsite or in geographically dispersed data centers.
3. **Data Encryption and Access Controls**
    - Encrypt all backup data at rest and in transit.
    - Restrict access to authorized IT personnel only.
4. **Retention and Disposal**
    - Follow regulatory and business requirements for retention (e.g., 7 years for financial records).
    - Securely erase outdated or obsolete backup data.
5. **Backup Verification and Testing**
    - Conduct monthly restore tests to verify backup integrity and completeness.
    - Monitor backup logs for errors or failures daily.
6. **Disaster Recovery**
    - Maintain updated disaster recovery documentation and contact lists.
    - Test recovery procedures bi-annually.

## 6. Documentation and Review

- Document all backup activities, issues, and restoration attempts.
- Review and update this SOP annually or following significant changes in IT infrastructure.

## 7. References

- [Relevant standards, e.g., ISO/IEC 27001, NIST SP 800-34]
- [Organizational policies]

## 8. Record of Changes

| Date | Version | Description | Owner |
|---|---|---|---|
| [YYYY-MM-DD] | 1.0 | Initial Release | [Name/Role] |