SOP: Secure Data Storage, Backup, and Recovery Guidelines

This SOP provides comprehensive **secure data storage, backup, and recovery guidelines** to ensure the protection, integrity, and availability of organizational data. It covers best practices for data encryption, access controls, regular backup schedules, offsite backup storage, and procedures for data recovery in case of data loss or corruption. The goal is to minimize risks associated with data breaches, hardware failures, and other incidents while maintaining compliance with relevant data protection regulations.

1. Purpose

To define and formalize procedures to securely store, back up, and recover organizational data, ensuring availability, integrity, and confidentiality.

2. Scope

This SOP applies to all employees, contractors, and third parties who access, manage, or store organizational data, regardless of storage location or medium.

3. Responsibilities

- **IT Team:** Implement and monitor backup and recovery processes.
- **Data Owners:** Identify data that requires protection and backup.
- **All Users:** Store data in approved storage systems only; report incidents promptly.

4. Secure Data Storage Guidelines

1. **Data Classification:** Classify data based on sensitivity and criticality.
2. **Encryption:**
    - Encrypt sensitive and confidential data at rest and in transit using approved algorithms (e.g., AES-256).
3. **Access Controls:**
    - Enforce least privilege principles; implement strong authentication and role-based access.
    - Periodically review and update access privileges.
4. **Physical Security:**
    - Ensure physical storage locations are restricted and monitored.

5. Data Backup Guidelines

1. **Backup Frequency:**
    - Critical data: Daily backups
    - Non-critical data: Weekly backups
2. **Backup Types:**
    - Full, incremental, and differential backups as per data criticality.
3. **Offsite/Cloud Backups:**
    - Maintain at least one backup copy offsite or in a secure cloud environment.
4. **Backup Retention:**
    - Retain backups according to organizational data retention policies and compliance requirements.
5. **Backup Security:**
    - Encrypt backup data; ensure access to backups is restricted and logged.
6. **Backup Testing:**
    - Test backup restoration procedures at least quarterly to ensure effectiveness.

6. Data Recovery Procedures

1. Assess and categorize the data loss or corruption incident.
2. Notify relevant stakeholders and escalate as needed.
3. Restore the latest clean backup to affected systems.

4. Verify the integrity and completeness of restored data.
5. Document the incident and recovery steps taken.

7. Compliance and Monitoring

- Regularly review backup and recovery processes for compliance with applicable laws and regulations (e.g., GDPR, HIPAA).
- Perform periodic audits to verify adherence to this SOP.

8. Review & Revision

- This SOP will be reviewed annually or following any data breach, technology change, or regulatory updates.
- Document all revisions and keep historical copies.

9. Contact Information

Role	Name/Title	Contact
IT Manager	Jane Doe	itmanager@example.com
Data Protection Officer	John Smith	dpo@example.com

Approval & Document Control

Approved by: _____

Date: _____

Version: 1.0