# Standard Operating Procedure (SOP)

## Digital and Physical Records Storage and Backup Procedures

This SOP details the **digital and physical records storage and backup procedures**, covering the proper organization, secure storage, and systematic backup of both electronic and paper records. It includes guidelines for data classification, access control, regular backup schedules, offsite storage, disaster recovery plans, and compliance with relevant data protection regulations to ensure the integrity, confidentiality, and availability of all records.

### 1. Purpose

To establish standardized procedures for the storage and backup of digital and physical records, ensuring continued integrity, confidentiality, and accessibility.

### 2. Scope

This SOP applies to all staff handling organizational records, both paper-based and electronic, across all departments.

### 3. Responsibilities

- **Records Manager:** Oversees compliance and implementation.
- **IT Department:** Manages digital storage, backups, and restoration processes.
- **All Employees:** Must adhere to these procedures and report breaches or issues.

### 4. Definitions

| Term | Definition |
|---|---|
| Digital Records | Data stored electronically, e.g., documents, emails, databases. |
| Physical Records | Paper-based materials such as files, printed reports, forms. |
| Backup | Copying and archiving of data for recovery in case of loss or damage. |

### 5. Procedure

#### 5.1 Data Classification

- Categorize data as *Public*, *Internal*, *Confidential*, or *Restricted*.
- Apply appropriate storage and access controls based on classification.

#### 5.2 Digital Records Storage

- Store digital files on secure, access-controlled servers or cloud solutions.
- Implement strong password policies and multi-factor authentication.
- Ensure regular software and security updates.

#### 5.3 Physical Records Storage

- File documents in clearly labeled, fire-resistant cabinets.
- Limit access to authorized personnel only.
- Store highly confidential records in separate, locked locations.

#### 5.4 Backup Procedures

- Schedule daily automated digital backups to primary onsite and secondary offsite locations.
- Back up critical physical records by digitization whenever possible and store copies offsite.
- Test backups monthly to ensure data integrity and retrievability.

#### 5.5 Offsite Storage

- Use accredited service providers for offsite storage of both digital and physical backups.
- Maintain detailed inventories and chain-of-custody records.

### 5.6 Disaster Recovery

- Develop and maintain a disaster recovery plan for both physical and digital records.
- Conduct annual recovery drills and update plans as needed.
- Ensure all key personnel have access to recovery protocols.

### 5.7 Compliance & Audit

- Ensure compliance with applicable data protection regulations (e.g., GDPR, HIPAA).
- Conduct regular audits of storage and backup practices.
- Document and address any incidents or breaches promptly.

## 6. Document Control

| Version | Date | Prepared by | Approved by | Change Description |
|---|---|---|---|---|
| 1.0 | 2024-06-13 | Records Manager | Management | Initial Release |