SOP: Secure Storage Protocols for Physical and Digital Records

This SOP details **secure storage protocols for physical and digital records**, encompassing guidelines for proper classification, access control, encryption methods, backup procedures, retention schedules, and disposal techniques. The objective is to protect sensitive information from unauthorized access, loss, or damage, ensuring data integrity and compliance with relevant regulations.

1. Scope

This SOP applies to all employees and contractors responsible for handling, storing, or managing physical and digital records within the organization, including sensitive, confidential, and proprietary information.

2. Responsibilities

- **Records Manager:** Oversee implementation and compliance.
- **IT Department:** Manage digital storage, encryption, and backups.
- **All Staff:** Adhere to protocols outlined in this SOP.

3. Definitions & Classification

Classification Level	Description	Examples
Public	Information intended for public disclosure.	Press releases, marketing materials.
Internal	Information for internal use only.	Policies, internal memos.
Confidential	Sensitive information requiring restricted access.	HR records, client information.
Restricted	Highly sensitive information with strictly limited access.	Financial reports, personal data, trade secrets.

4. Access Control

1. Grant access strictly based on job necessity (â€œneed to knowâ€ principle).
2. Maintain an up-to-date authorized access list for both physical and digital records.
3. Utilize secure authentication (passwords, badges, biometrics) for digital and physical access.
4. Log all access and review logs periodically for suspicious activities.

5. Secure Storage Protocols

a. Physical Records

- Store in locked cabinets or rooms with restricted access.
- Control environmental factors (fire, water, humidity).
- Install surveillance and alarm systems in high-security areas.
- Label sorted by classification.

b. Digital Records

- Store on secure, access-controlled servers or cloud platforms.
- Apply strong encryption (e.g., AES-256) for data at rest and in transit.
- Enable multi-factor authentication for system access.
- Regularly patch and update storage systems.

6. Backup Procedures

- Back up digital records daily using encrypted media.
- Store backups offsite or in a secure, geographically separated location.
- Test restoration procedures quarterly.
- Document backup schedules and responsible personnel.

7. Retention & Disposal

1. Follow legally mandated retention schedules for each record category.
2. Perform annual reviews and dispose of records past retention using approved secure methods.
3. **Disposal Techniques:**
    - **Physical:** Shredding, incineration.
    - **Digital:** Secure erasure, degaussing, physical destruction of storage media.

4. Maintain records of disposed items and responsible personnel.

8. Compliance & Monitoring

- Ensure all protocols meet applicable laws (GDPR, HIPAA, etc.) and industry standards.
- Conduct periodic audits and risk assessments.
- Document all breaches or protocol deviations and implement corrective actions.

9. Training & Awareness

- Provide onboarding and annual refresher training to all personnel handling records.
- Circulate updates to this SOP as needed, with staff acknowledgement.

10. Revision History

Date	Version	Changes	Author
2024-06-10	1.0	Initial version	Records Manager