SOP: Secure Document Storage and Access Control

This SOP details **secure document storage and access control** protocols, including proper classification and handling of sensitive documents, physical and digital storage security measures, access permission management, regular audits and monitoring, data encryption practices, and procedures for document retrieval and disposal. The objective is to protect confidential information, prevent unauthorized access, and ensure compliance with organizational and regulatory requirements.

1. Purpose

To establish standardized procedures for secure document storage and access, maintaining confidentiality, integrity, and availability of sensitive information.

2. Scope

This SOP applies to all employees, contractors, and third parties handling physical and digital documents within the organization.

3. Definitions

- **Confidential Documents**: Files containing sensitive, confidential, or regulated information.
- **Access Control**: Mechanisms that restrict access to files based on user roles/permissions.
- **Encryption**: Process of converting information into a secure format.

4. Document Classification and Handling

- Classify all documents as Public, Internal, Confidential, or Restricted.
- Label documents clearly according to their classification.
- Handle and distribute documents in compliance with classification label.

5. Physical Document Storage

- Store sensitive physical documents in locked cabinets or secure rooms with restricted access.
- Limit access to authorized personnel; maintain access logs.
- Ensure facilities have security systems (alarms, surveillance, badges, etc.).

6. Digital Document Storage

- Store digital documents on secure, encrypted servers or approved cloud platforms.
- Enable file-level encryption and regular backups.
- Restrict access using user authentication and role-based permissions.

7. Access Permission Management

- Grant access based on the principle of least privilege.
- Review and update access rights quarterly or as needed.
- Document all access changes and approvals.

8. Audits and Monitoring

- Conduct regular audits of document access logs and storage areas.
- Monitor for unauthorized access or unusual activity.
- Report and respond to security incidents according to IR procedures.

9. Data Encryption Practices

- Encrypt sensitive documents during storage and transmission.
- Use industry-standard encryption protocols and update them regularly.
- Safeguard encryption keys in a secure environment with restricted access.

10. Document Retrieval and Disposal

- Authorize retrieval requests; log each request and approval.
- Shred physical documents and use secure deletion methods for digital files upon disposal.
- Document all disposals for audit purposes.

11. Compliance & Training

- Train staff on SOP protocols and responsibilities annually.
- Review this SOP as regulations or organizational needs change, at least every two years.
- Ensure compliance with relevant laws (GDPR, HIPAA, etc.).

12. Responsibilities

Role	Responsibilities
Document Owner	Classify documents; authorize access
IT/Admin	Implement security controls; monitor access
All Staff	Comply with handling and storage protocols

13. Revision History

Date	Description	Author
YYYY-MM-DD	Initial Draft	[Name]