Standard Operating Procedure (SOP)
Secure Document Storage and Filing Protocols

1. Purpose

This SOP defines the **secure document storage and filing protocols** to ensure the protection, organization, and easy retrieval of sensitive and important documents. It covers guidelines for document classification, confidential handling procedures, access control measures, physical and electronic storage standards, regular audits, and retention schedules. The objective is to maintain document integrity, prevent unauthorized access, and comply with relevant legal and regulatory requirements.

2. Scope

This SOP applies to all personnel, contractors, and stakeholders who handle, store, or access organizational documents, both in physical and electronic formats.

3. Responsibilities

- **Document Owner:** Classifies and determines access rights for documents.
- **All Staff:** Comply with handling, storage, and access protocols.
- **IT Department:** Maintains digital storage security and access logs.
- **Records Manager:** Oversees retention schedules and conducts audits.

4. Document Classification

Classification Level	Description
Public	Information approved for unrestricted disclosure.
Internal	Information limited to staff or specific stakeholders.
Confidential	Sensitive information restricted to authorized personnel only.
Restricted	Highly sensitive, critical, or legally protected documents.

5. Secure Handling Procedures

- Label documents clearly with the appropriate classification level.
- Handle confidential/restricted documents in accordance with organization's data protection policies.
- Prohibit removal of sensitive documents from secured areas without authorization.

6. Access Controls

- Grant access based on the principle of least privilege.
- Maintain access logs for physical and electronic records.
- Regularly review and update access permissions.

7. Physical Storage Standards

- Store sensitive documents in locked cabinets or secured rooms with controlled access.
- Ensure storage areas are protected from fire, water, and environmental damage.
- Restrict storage area keys/cards to authorized personnel only.

8. Electronic Storage Standards

- Store electronic documents on secure, backed-up servers or cloud storage compliant with data protection standards.

- Encrypt confidential and restricted documents in transit and at rest.
- Implement multi-factor authentication for access to restricted files/systems.

9. Audits and Monitoring

- Conduct periodic audits of storage systems and access logs.
- Review compliance with storage and handling procedures.

10. Document Retention and Disposal

- Maintain documents in accordance with legal, regulatory, and business requirements.
- Follow retention schedules for each document type.
- Securely dispose of documents past their retention period using shredding or certified electronic deletion.

11. Compliance and Review

- Ensure adherence to all applicable laws, regulations, and organizational policies.
- Review and update the SOP annually or as required by changing regulations or organizational needs.

12. References

- Applicable data protection laws and regulations
- Organization's Information Security Policy