SOP: Secure Storage and Filing Requirements

This SOP details the **secure storage and filing requirements**, covering guidelines for the proper organization, protection, and management of sensitive documents and records. It includes procedures for secure physical storage, digital filing systems, access control, confidentiality measures, retention periods, and disposal protocols to ensure data integrity and prevent unauthorized access.

1. Purpose

To establish standardized requirements and responsibilities for the secure storage, organization, access, retention, and disposal of sensitive documents and records.

2. Scope

This SOP applies to all employees and contractors who create, access, manage, or dispose of sensitive documents (both physical and electronic) within the organization.

3. Definitions

- **Sensitive Documents**: Materials containing proprietary, personal, or confidential information requiring protection from unauthorized access.
- **Physical Storage**: Filing cabinets, safes, or storage areas for paper records.
- **Digital Filing System**: Cloud-based or internal server systems for managing electronic records.

4. Responsibilities

- **All Staff**: Ensure compliance with this SOP whenever handling sensitive documents.
- **Managers/Supervisors**: Monitor staff adherence and report any breaches.
- **IT Department**: Maintain secure digital systems and support access control measures.

5. Procedures

Process	Procedure
5.1 Physical Storage	• Store documents in locked, fireproof cabinets or safes located in a secure area. • Limit access to authorized personnel only (issue keys or entry codes as needed). • Maintain an access log for entry to physical document storage areas.
5.2 Digital Filing Systems	• Store electronic files on secure, access-controlled servers or trusted cloud platforms. • Implement user authentication (e.g., strong passwords, two-factor authentication). • Ensure all sensitive files are regularly backed up and encrypted.
5.3 Access Control & Confidentiality	• Assign access rights based on defined roles and the need-to-know principle. • Review and update access permissions regularly. • Prohibit unauthorized reproduction, sharing, or removal of sensitive documents.

Process	Procedure
5.4 Retention Periods	• Follow company policy and legal/regulatory guidelines regarding document retention timelines. • Maintain a retention schedule for all document categories. • Review and archive or dispose of records once retention periods expire.
5.5 Secure Disposal	• Physically shred paper documents using a cross-cut shredder when disposal is authorized. • Permanently delete electronic files from all digital storage locations and backups. • Use certified confidential waste disposal services as required. • Document all disposals (log date, document type, and authorized personnel).

6. Breach Reporting

- Immediately report any suspected or actual breaches in security or confidentiality to the information security officer/manager.
- Document the incident and corrective actions taken.

7. Review and Revision

- This SOP shall be reviewed biennially or as required following major security incidents, regulatory changes, or technological upgrades.

8. Related Documents

- Information Security Policy
- Access Control Policy
- Data Retention & Disposal Policy

Document Owner: [Your Department/Officer Name]
Reviewed: [Date]
Next Review Due: [Date]