SOP Template
Physical and Digital File Storage Location Guidelines

This SOP outlines the **physical and digital file storage location guidelines**, including the categorization of files, secure storage practices, access control measures, backup protocols, retention periods, and disposal procedures. The purpose is to ensure the efficient organization, protection, and retrieval of important documents while maintaining data integrity and compliance with regulatory standards.

1. Scope

This procedure covers all physical and digital files created, received, and maintained by the organization.

2. Categorization of Files

- Administrative
- Financial
- Legal
- HR/Personnel
- Operational
- Confidential/Sensitive
- Other (specify as required)

Each file must be labeled and categorized appropriately upon creation/receipt.

3. Physical File Storage Guidelines

- Store files in designated, clearly labeled cabinets or shelves.
- Use lockable cabinets for confidential/sensitive documents.
- Restrict storage access to authorized personnel only.
- Ensure storage areas are protected from fire, water, pests, and unauthorized entry.
- Maintain a register of stored files, including their location and access history.

4. Digital File Storage Guidelines

- Store files on secure, access-controlled servers/cloud platforms approved by IT.
- Organize files using standardized folder structures and naming conventions.
- Password-protect confidential or sensitive documents.
- Apply encryption to particularly sensitive files as necessary.
- Update and review digital storage locations regularly for proper organization and redundancy.

5. Access Control Measures

- Only authorized individuals may access, modify, or remove files.
- Maintain access logs for both physical and digital records.
- Conduct periodic reviews of user access permissions.
- Immediately update permissions upon staff role changes or departures.

6. Backup Protocols

- For digital files, implement daily automated backups to a secure, offsite location.
- Test backup restoration procedures at least quarterly.
- Physical files: Digitize and back up critical documents whenever possible.
- Store backup copies access-restricted and security-monitored.

7. Retention Periods

Category	Retention Period
Administrative	3 years
Financial	7 years
Legal	Indefinite or as required by law
HR/Personnel	7 years after employee departure
Operational	5 years
Confidential/Sensitive	As specified by contract/regulation

Review and update retention periods as dictated by regulatory or organizational changes.

8. Disposal Procedures

- Shred paper files approved for disposal to prevent data reconstruction.
- Permanently delete digital files using secure erasure methods.
- Document all disposals with date, file description, method, and responsible personnel.
- Ensure disposal is witnessed or verified according to sensitivity level.

9. Compliance and Review

- Staff must adhere to this SOP and applicable legal/regulatory requirements.
- Conduct annual reviews of file storage, access controls, and backup/restoration effectiveness.
- Revise SOP as needed based on audit findings, incidents, or regulatory changes.

10. References

- Company Information Security Policy
- Data Protection Laws & Regulations (e.g., GDPR, HIPAA)
- Industry or contractual requirements
- Related SOPs

11. Document Control

Version	Date	Author	Approval
1.0	2024-06-27	[Author Name]	[Approver Name/Signature]