Standard Operating Procedure (SOP): Digital Document Scanning and Storage Protocols

Purpose: This SOP details **digital document scanning and storage protocols**, including guidelines for document preparation, scanning resolution and format standards, file naming conventions, metadata tagging, secure digital storage solutions, backup and data recovery procedures, access control and permissions, regular audit and maintenance schedules, and compliance with data protection regulations. The objective is to ensure efficient, accurate, and secure management of digital documents for easy retrieval and long-term preservation.

1. Document Preparation

1. Remove paper clips, staples, and bindings.
2. Arrange documents in order and ensure pages are not torn or folded.
3. Clean documents if necessary to ensure optimal scan quality.
4. Label each document batch with relevant identification information.

2. Scanning Standards

1. Set scanner resolution to a minimum of **300 DPI** for standard documents; **600 DPI** for images or archival materials.
2. Preferred file formats: **PDF/A** for textual documents, **TIFF** or **JPEG** for images.
3. Scan in color or grayscale as required.
4. Ensure all scanned pages are legible and complete.

3. File Naming Conventions

1. Adopt a consistent naming format: `YYYYMMDD_Department_DocumentType_Description_Version.pdf`
2. Avoid spaces and special characters; use underscores or hyphens.

Component	Example
Date	20240614
Department	FIN
Document Type	Invoice
Description	VendorName
Version	v1

4. Metadata Tagging

1. Tag each digital file with metadata including title, author, date, department, and keywords for efficient search and retrieval.
2. Use document management system (DMS) metadata fields when uploading files.

5. Secure Digital Storage Solutions

1. Store scanned documents in a secure, access-controlled repository (cloud or on-premises DMS).
2. Organize storage hierarchically (e.g., by year, department, document type).
3. Ensure all storage solutions meet organizational security standards (encryption at rest and in transit).

6. Backup and Data Recovery

1. Implement automated daily backups to secondary and offsite locations.
2. Test data recovery capability at least quarterly to ensure backup integrity.
3. Document backup and recovery procedures, including response times and responsible personnel.

7. Access Control and Permissions

1. Grant system access based on defined roles and responsibilities.
2. Review permissions regularly, especially after staff changes.
3. Audit logs of document access and modifications.

8. Audit and Maintenance Schedule

1. Conduct semi-annual audits of digital document repositories for completeness, accuracy, and compliance.
2. Verify document readability, metadata accuracy, and file integrity.
3. Update and maintain SOP as required by changes in regulations or technology.

9. Compliance with Data Protection Regulations

1. Adhere to relevant local and international data protection laws (e.g., GDPR, HIPAA).
2. Maintain records of consent and data processing as required.
3. Report data breaches immediately according to organizational protocols.

10. Revision History

Date	Version	Description of Change	Author
2024-06-14	1.0	Initial creation	[Name]