SOP: Electronic and Physical Document Segregation Instructions

This SOP provides detailed **electronic and physical document segregation instructions** to ensure proper organization, secure storage, and efficient retrieval of documents. It covers the classification criteria for different document types, guidelines for separating sensitive and non-sensitive information, methods for maintaining the integrity and confidentiality of records, and procedures for managing both digital files and hard copies. The objective is to enhance document management practices, minimize risks of data loss or unauthorized access, and comply with organizational and regulatory requirements.

1. Purpose

To establish standardized procedures for segregating, organizing, and managing both electronic and physical documents, ensuring confidentiality, integrity, ease of retrieval, and compliance with regulations.

2. Scope

This SOP applies to all staff responsible for handling organizational records in both digital and physical formats.

3. Document Classification

Classification	Examples	Access Level
Sensitive/Confidential	Personnel files, financial records, client data	Authorized personnel only
Internal Use	Meeting notes, project documentation	Internal staff
Public	Marketing materials, press releases	Open

4. Segregation Instructions

4.1 Electronic Documents

- Store sensitive and non-sensitive documents in separate, clearly labeled folders or document management systems (DMS).
- Apply access controls and permissions based on classification.
- Use encryption for confidential electronic files.
- Maintain regular backups in secure, segregated storage locations.
- Log all access and modifications to sensitive documents.

4.2 Physical Documents

- Segregate sensitive physical documents in locked filing cabinets or secure storage rooms.
- Label storage containers clearly to indicate classification level.
- Limit access to authorized personnel only; maintain an access log.
- Store non-sensitive documents separately in general filing areas.
- Implement a check-out/check-in system for highly sensitive records.

5. Integrity and Confidentiality Measures

- Restrict permissions and regularly review access lists for both formats.
- Use tamper-evident seals for confidential hard copies.
- Encrypt digital files and use password-protected archives where required.
- Shred or securely delete documents upon retention period expiry following an approved destruction protocol.

6. Document Retrieval and Tracking

- Maintain an indexed inventory (manual or digital) of both physical and electronic documents.
- Apply version controls to electronic records; date-stamp all physical files.

- Record retrieval details for sensitive files (who, when, and purpose).
- Audit document storage and segregation procedures annually.

7. Regulatory Compliance

- Ensure procedures align with applicable laws, standards, and internal policies (e.g., GDPR, HIPAA, ISO 27001).
- Document all segregation, access, and destruction activities for audit readiness.

8. Roles and Responsibilities

- **Records Manager:** Oversee implementation and review of segregation practices.
- **IT Department:** Manage electronic segregation, backups, and access controls.
- **All Staff:** Adhere to segregation guidelines and immediately report any breaches or concerns.

9. Review and Updates

This SOP should be reviewed annually or upon significant organizational or regulatory changes. Updates must be approved and communicated to all relevant personnel.