SOP: Record-keeping, Archiving, and Data Privacy Standards

This SOP defines the **record-keeping, archiving, and data privacy standards**, establishing protocols for accurate documentation, secure storage, systematic archiving, and protection of sensitive information. It ensures compliance with legal requirements, promotes data integrity, safeguards confidentiality, and facilitates efficient retrieval of records while minimizing risks related to unauthorized access or data loss.

1. Purpose

To establish standardized procedures for record-keeping, archiving, and maintaining data privacy, ensuring data integrity, security, and legal compliance.

2. Scope

This SOP applies to all staff handling organizational or client records (physical or digital) and to any information classified as confidential, personal, or sensitive.

3. Definitions

Term	Definition
Record	Any document, file, or data (physical or digital) created or received in the course of operations.
Archiving	The process of storing inactive records securely for long-term retention and future reference.
Data Privacy	Practices and policies designed to protect personal, private, or sensitive information from unauthorized access or disclosure.
Retention Period	Amount of time a record must be kept before eligible for destruction or deletion.

4. Responsibilities

- **All Staff:** Properly handle, store, and archive records as per this SOP.
- **Records Manager/Data Protection Officer:** Oversee implementation, review compliance, conduct training, and coordinate audits.
- **IT Department:** Maintain secure digital storage and backup systems; monitor access and data integrity.

5. Procedures

5.1 Record Creation & Documentation

1. Document all activities, transactions, or communications according to departmental requirements.
2. Ensure documentation is clear, accurate, complete, and timestamped.
3. Classify records by type (e.g., financial, personnel, client-related) and sensitivity (public, internal, confidential).

5.2 Storage & Security

- Store physical records in locked, access-controlled areas.
- Store electronic records on secure, password-protected systems with regular backups.
- Restrict access to authorized personnel only.
- Encrypt sensitive data during storage and transmission.

5.3 Archiving

1. Archive records that are not required for daily operations but need to be retained per the retention schedule.
2. Document the transfer to archives, noting location, type, date, and responsible person.
3. Store archives in secure but accessible locations (off-site or digital vaults, as applicable).

5.4 Retention & Disposal

- Records must be retained for the period specified by legal, regulatory, or contractual requirements.
- Review records periodically for eligibility for destruction.
- Destroy records securely-shred physical documents, permanently delete digital files. Maintain logs of all disposals.

5.5 Data Privacy Standards

1. Collect and use personal/sensitive data strictly for authorized purposes.
2. Obtain consents where legally required and maintain confidentiality agreements.
3. Respond promptly to requests for access, correction, or deletion of personal data.
4. Report data breaches immediately to the Data Protection Officer and follow incident response procedures.

6. Compliance & Audits

- Periodic audits must be conducted to ensure adherence to record-keeping, archiving, and data privacy standards.
- Non-compliance will result in corrective action and potential disciplinary measures.

7. References

- Applicable data protection laws (e.g., GDPR, HIPAA, national/local regulations)
- Company-specific policies and retention schedules

8. Revision History

Version	Date	Description of Change	Author
1.0	2024-06-08	Initial SOP template created	AI Assistant