SOP: Documentation and Record-Keeping of Confidential Data Activities

This SOP details the procedures for **documentation and record-keeping of confidential data activities**, encompassing the accurate recording, secure storage, and controlled access of sensitive information. It ensures compliance with data protection regulations, promotes data integrity, and supports audit readiness by defining roles, responsibilities, retention periods, and protocols for handling confidential records throughout their lifecycle.

1. Purpose

To establish standardized procedures for documenting, securely storing, accessing, retaining, and disposing of records pertaining to confidential data activities.

2. Scope

This SOP applies to all personnel who create, access, manage, or store confidential data within the organization.

3. Definitions

Term	Definition
Confidential Data	Any information classified as confidential by law, regulation, or internal policy (e.g., personal data, financial data, proprietary information).
Record	Any document or data (physical or electronic) that evidences actions, events, or decisions related to confidential data.
Data Owner	Individual responsible for the data's proper management and protection.

4. Roles and Responsibilities

- **Data Owner:** Ensure appropriate classification, documentation, storage, and authorized access.
- **IT/Records Management:** Implement and maintain secure storage solutions; oversee access controls and retention schedules.
- **Data Users:** Accurately document activities, follow SOP, and report suspected breaches.
- **Compliance Officer:** Monitor data handling practices and audit record-keeping activities for regulatory compliance.

5. Procedures

1. **Documentation of Activities**
    - Accurately record activities involving confidential data (e.g., creation, access, transfer, destruction) using designated forms or electronic logs.
    - Include date/time, nature of activity, personnel involved, and purpose.
2. **Secure Storage of Records**
    - Store physical records in locked cabinets; restrict access to authorized personnel only.
    - Store electronic records in secure, access-controlled systems with encryption enabled.
3. **Controlled Access**
    - Grant access based on role and necessity; review access rights at least annually or upon changes in personnel roles.
    - Log all access to confidential data records for audit purposes.
4. **Retention and Disposal**
    - Retain records for periods specified by legal, regulatory, or internal requirements.
    - Securely destroy records past retention using approved shredding or data wiping procedures.
5. **Incident Reporting**
    - Report any unauthorized access, loss, or breach of confidential records immediately to the Compliance Officer.

6. Audit and Review

- Conduct periodic audits of documentation practices, storage integrity, and access logs.
- Update this SOP in response to regulatory, technological, or organizational changes.

7. References

- Relevant data protection regulations (e.g., GDPR, HIPAA)
- Internal data classification and retention policies

8. Revision History

Date	Version	Description	Author
2024-06-01	1.0	Initial SOP Release	[Your Name]