SOP: Secure Documentation, Record-Keeping, and Data Privacy Procedures

1. Purpose

This SOP defines the procedures for **secure documentation, record-keeping, and data privacy** to ensure the confidentiality, integrity, and availability of sensitive information. It covers document classification, secure storage methods, authorized access controls, data retention policies, regular audits, and compliance with relevant privacy laws and regulations. The goal is to protect organizational data from unauthorized access, loss, or misuse while maintaining accurate and accessible records for operational and legal purposes.

2. Scope

This SOP applies to all organizational records and documentation, including physical and electronic records, involving employees, clients, vendors, or partners.

3. Definitions

Term	Definition
Confidential Data	Any information designated as sensitive, requiring restricted access.
Record-Keeping	The systematic control of records throughout their lifecycle.
Data Privacy	The handling of data in compliance with applicable privacy laws and regulations.

4. Responsibilities

- **All Staff:** Adhere to SOP requirements regarding documentation handling and data privacy.
- **Data Protection Officer:** Oversee implementation and compliance; conduct audits.
- **Managers/Supervisors:** Ensure team compliance and provide training.

5. Procedures

5.1 Document Classification

1. Classify documents as *Confidential*, *Internal Use*, or *Public* per organizational policy.
2. Label each document accordingly (header/footer for digital, stamp for physical).

5.2 Secure Storage Methods

1. Physical files must be stored in locked cabinets within secure areas.
2. Electronic documents stored on secure, access-controlled servers with regular backups.
3. Use encryption for sensitive electronic records both at rest and in transit.

5.3 Authorized Access Controls

1. Restrict access to sensitive documents based on role and necessity.
2. Access permissions to be reviewed and updated bi-annually or upon role changes.
3. Require strong password protection and multi-factor authentication for access to electronic records.

5.4 Data Retention & Disposal

1. Follow the data retention schedule: retain documents only as long as necessary per legal and business requirements.
2. Securely dispose of records (shredding for physical, secure deletion for electronic).
3. Document all disposal actions with date, type of record, and method.

5.5 Regular Audits & Monitoring

1. Perform annual audits of access logs, retention schedules, and storage security.
2. Document findings and implement corrective actions as needed.

5.6 Compliance with Laws & Regulations

1. Ensure all handling aligns with applicable privacy laws (e.g., GDPR, HIPAA).
2. Train staff annually on data protection and regulatory requirements.

6. Documentation & Training

- Maintain and regularly update records of SOP training and policy acknowledgments.
- Staff must acknowledge receipt and understanding of SOP annually.

7. Incident Response

1. Immediately report suspected data breaches to the Data Protection Officer.
2. Follow the incident response plan to contain, assess, and remediate the breach.
3. Document all incident details and corrective actions.

8. Revision History

Version	Date	Description	Author
1.0	2024-06-10	Initial Template	[Your Name/Title]

All employees are responsible for familiarizing themselves with and adhering to this SOP.