Standard Operating Procedure (SOP): Management of Confidential and Sensitive Information

This SOP details the **management of confidential and sensitive information**, covering data classification, secure storage and access controls, proper handling and sharing protocols, data encryption standards, employee responsibilities, breach response procedures, and compliance with relevant privacy laws and regulations. The objective is to protect sensitive information from unauthorized access, disclosure, or loss, ensuring organizational integrity and maintaining stakeholder trust.

1. Purpose

To outline procedures for the identification, management, and protection of confidential and sensitive information within the organization, ensuring compliance with legal and regulatory requirements.

2. Scope

This SOP applies to all employees, contractors, and third parties who access, process, or handle the organization's confidential and sensitive information.

3. Definitions

Term	Definition
Confidential Information	Information that, if disclosed, could cause harm to the organization or individuals (e.g., financial data, customer records, intellectual property).
Sensitive Information	Personal or private data that requires additional protection due to privacy or legal requirements (e.g., PII, health records).
PII	Personally Identifiable Information

4. Data Classification

1. Identify and classify data into categories: Public, Internal, Confidential, and Restricted.
2. Review data classification regularly and update as necessary.
3. Label documents and systems accordingly.

5. Secure Storage and Access Controls

1. Store confidential and sensitive data in authorized, secure locations (e.g., encrypted drives, password-protected cabinets, secure cloud services).
2. Restrict access based on job roles and responsibilities using the principle of least privilege.
3. Use access logs and regular audits to monitor data access activities.

6. Handling and Sharing Protocols

1. Share confidential/sensitive information on a need-to-know basis only.
2. Transmit sensitive information using secure methods (encrypted email, secure file transfer).
3. Verify recipient identities before sharing.
4. Keep physical documents secure; shred when no longer needed.

7. Data Encryption Standards

1. Encrypt data at rest and in transit using industry-standard protocols (e.g., AES-256, TLS 1.2+).
2. Update cryptographic keys regularly and manage them securely.

8. Employee Responsibilities

1. Complete mandatory information security training annually.
2. Report any suspicious activities or potential breaches without delay.
3. Comply with all relevant data protection policies and procedures.

9. Breach Response Procedures

1. Immediately report suspected or actual data breaches to IT/security management.
2. Contain and assess the impact of the breach following the incident response plan.
3. Notify affected parties and regulatory authorities as required by law.
4. Document lessons learned and update procedures accordingly.

10. Compliance

1. Adhere to all relevant laws and regulations (e.g., GDPR, HIPAA, local data protection acts).
2. Conduct periodic compliance reviews and risk assessments.

11. Review and Revision

This SOP shall be reviewed annually or upon significant change in relevant regulations, processes, or systems. All revisions must be documented and communicated to staff.

12. Document Control

Version	Date	Author	Change Description
1.0	2024-06-30	Policy Owner	Initial release