# Standard Operating Procedure (SOP): Confidentiality and Privacy Management

This SOP establishes guidelines for **confidentiality and privacy management**, encompassing the proper handling, storage, and sharing of sensitive information. It defines roles and responsibilities, data access controls, secure communication protocols, compliance with applicable privacy laws, breach response procedures, and employee training requirements. The objective is to protect personal and organizational data from unauthorized disclosure and ensure trust and compliance throughout all operations.

## 1. Purpose

To ensure the confidentiality, integrity, and privacy of sensitive information by establishing standards and procedures for its management throughout all business operations.

## 2. Scope

This SOP applies to all employees, contractors, and third-party vendors who handle or access confidential or personal data controlled by the organization.

## 3. Roles and Responsibilities

| Role | Responsibilities |
|---|---|
| Data Owner | Define data classification, authorize access, and ensure proper use of data. |
| Data Custodian | Implement and maintain data controls as defined by the data owner. |
| Employees | Handle information according to this SOP and complete required privacy training. |
| IT/Security Team | Implement technical controls for data access, storage, and transmission; monitor and respond to security incidents. |
| Compliance Officer | Oversee adherence to applicable data privacy laws and regulations. |

## 4. Data Access Controls

- Grant access to confidential data strictly on a need-to-know basis.
- Implement authentication (e.g., strong passwords, multi-factor authentication) and authorization mechanisms.
- Review and update access rights regularly and upon role changes or terminations.

## 5. Secure Handling, Storage, and Sharing

- Store sensitive information in encrypted formats using approved solutions.
- Prohibit storage of confidential information on unauthorized personal devices or cloud services.
- Transmit sensitive data only via secure, encrypted communication channels (e.g., TLS/SSL, secure file transfer).
- Maintain a clear desk and screen policy to reduce risk of inadvertent exposure.
- Share confidential information externally only with prior authorization and under a non-disclosure agreement (NDA).

## 6. Compliance with Privacy Laws and Regulations

- Adhere to relevant privacy laws (e.g., GDPR, CCPA, HIPAA) and organizational policies.
- Conduct periodic risk and compliance assessments.
- Maintain records of data processing activities as required by law.

## 7. Breach Response Procedures

- Immediately report suspected or actual breaches to the IT/Security team and Compliance Officer.
- Contain, assess, and document the breach following the incident response plan.
- Notify affected individuals and authorities as required by law or policy.
- Conduct post-incident reviews to improve processes and prevent recurrence.

## 8. Employee Training and Awareness

- All employees must complete mandatory confidentiality and privacy training upon hire and annually thereafter.
- Provide targeted training after relevant policy changes or incidents.
- Regularly communicate best practices and reminders concerning data security.

## 9. Document Control

| Version | Date | Author | Approval |
|---|---|---|---|
| 1.0 | 2024-06-27 | [Author Name] | [Approver Name] |