Standard Operating Procedure (SOP)
Handling of Confidential and Sensitive Mail

This SOP details the **handling of confidential and sensitive mail** instructions, encompassing proper identification, secure receiving, careful processing, and strict distribution protocols. It emphasizes maintaining privacy, preventing unauthorized access, ensuring timely delivery, and adhering to compliance standards to protect sensitive information and uphold organizational security policies.

1. Purpose

To establish standardized procedures for identifying, receiving, processing, and distributing confidential and sensitive mail to safeguard sensitive information and ensure organizational compliance and security.

2. Scope

This SOP applies to all employees and departments responsible for handling confidential and sensitive mail within the organization.

3. Definitions

- **Confidential Mail:** Mail containing information restricted to specific individuals or departments, including personnel records, legal documents, or financial data.
- **Sensitive Mail:** Mail that, if disclosed, could result in privacy breaches, security threats, or organizational harm.

4. Responsibilities

- **Mailroom Staff:** Ensure proper identification, logging, secure storage, and processing of confidential and sensitive mail.
- **Recipients:** Promptly receive, acknowledge, and securely store sensitive or confidential mail.
- **Supervisors/Managers:** Oversee adherence to this SOP and address any breaches or incidents.

5. Procedures

1. **Identification**
    - Look for markings such as "Confidential", "Sensitive", "Private", or "Addressee-only".
    - If unsure, treat ambiguous mail as sensitive.
2. **Receiving**
    - Log the receipt of confidential and sensitive mail in a secure record (manual or electronic).
    - Store in a locked cabinet or designated secure holding area until processing.
3. **Processing**
    - Open only if authorized. Preferably, deliver unopened to the addressee.
    - Avoid leaving mail unattended or in open areas.
    - Handle with clean hands and avoid marks or damage to the mail contents.
4. **Distribution**
    - Deliver confidential/sensitive mail directly to the named addressee or their authorized representative, requiring a signature if necessary.
    - Do not leave confidential mail in public or shared spaces.
5. **Record Keeping**
    - Maintain a confidential mail log, including date, recipient, and delivery details.
    - Retain records securely as per the organization's data retention policy.
6. **Incident Reporting**
    - **Immediately report any suspected or confirmed breaches, loss, or tampering to management and security/IT teams.**

6. Compliance

Follow company privacy policies, data protection regulations (e.g., GDPR, HIPAA), and any other legal requirements specific to handling confidential information.

7. Training

All personnel handling mail should be trained in these procedures and undergo periodic refresher training.

8. Revision History

Version	Date	Description	Author
1.0	2024-06-XX	Initial SOP release	[Author Name]