

Standard Operating Procedure (SOP)

Guidelines for Confidential and Sensitive Mail Handling

This SOP details **guidelines for confidential and sensitive mail handling**, covering the proper procedures for receiving, sorting, distributing, and securely storing confidential correspondence. It emphasizes the importance of maintaining privacy, preventing unauthorized access, handling sensitive information with discretion, and ensuring compliance with organizational policies and legal requirements to protect the integrity and confidentiality of all mail items.

1. Purpose

To establish standardized procedures for handling mail classified as confidential or sensitive, ensuring the integrity, privacy, and protection of correspondence from unauthorized access or disclosure.

2. Scope

This procedure applies to all employees, contractors, and temporary staff responsible for receiving, processing, distributing, and storing organizational mail and packages identified as confidential or sensitive.

3. Responsibilities

- **Mailroom Staff:** Adhere to guidelines for secure handling, sorting, and distribution of confidential mail.
- **Managers/Supervisors:** Ensure personnel are trained and policies are enforced.
- **All Employees:** Maintain confidentiality and follow procedures upon receiving sensitive mail.

4. Procedures

1. **Receiving Mail:**
 - Inspect all mail for external markings indicating confidentiality (e.g., "Confidential," "Personal," or "Private").
 - Log confidential items in a secure mail register or tracking system.
2. **Sorting Mail:**
 - Sort confidential mail separately from general correspondence.
 - Store in a secure, access-controlled location until distribution.
3. **Distributing Mail:**
 - Deliver confidential mail directly to the intended recipient or authorized delegate only.
 - Require recipient signature upon delivery for sensitive items.
4. **Secure Storage:**
 - Store undelivered confidential mail in a locked cabinet or safe with restricted access.
 - Implement regular audits and access reviews for mail storage areas.
5. **Destruction of Mail:**
 - Shred or securely dispose of returned, unclaimed, or obsolete confidential mail according to organizational policies.

5. Privacy and Security

- Do not disclose mail contents or recipients to unauthorized individuals.
- Report any suspected breach of mail security to management immediately.
- **Always comply with organizational policies and relevant legal/regulatory requirements regarding confidentiality.**

6. Training

All staff handling confidential mail must complete annual privacy and information security training and review this SOP periodically.

7. Review and Revision

This SOP must be reviewed at least annually or whenever significant changes in mail handling procedures or applicable laws occur.

8. References

- Organizational Privacy Policy
- Information Security Standards
- Relevant Data Protection Laws (e.g., GDPR, HIPAA)