SOP: Record-keeping, Documentation, and Communication Standards

This SOP defines the **record-keeping, documentation, and communication standards** necessary for maintaining accurate, consistent, and secure records. It covers procedures for data entry, document management, information sharing, confidentiality protocols, and regular auditing to ensure compliance with regulatory requirements and organizational policies. The goal is to enhance transparency, traceability, and effective communication across all departments.

1. Purpose

To establish standardized procedures for record-keeping, documentation, and communication across the organization, ensuring information is accurate, secure, and accessible as required.

2. Scope

This SOP applies to all personnel, departments, records, and communication channels within the organization.

3. Responsibilities

- **Department Heads**: Oversee implementation within their teams.
- **Employees**: Comply with the procedures outlined in this SOP.
- **Records Officer/Administrator**: Maintain records, conduct audits, and ensure compliance.
- **IT Department**: Maintain secure digital infrastructure for record-keeping and communication.

4. Procedures

4.1 Data Entry

- All records must be entered promptly and accurately into designated systems (paper or digital).
- Entries must include date, time, responsible person, and relevant reference numbers where applicable.
- Correct errors by recording corrections and maintaining an audit trail; do not erase or overwrite original data.

4.2 Document Management

- Store documents in approved locations (locked filing cabinets for paper; secure drives/cloud for digital).
- Use consistent naming conventions and version control for digital files.
- Retain documents according to the organization's retention schedule; archive or securely destroy when retention period ends.
- Restrict access to authorized personnel only.

4.3 Information Sharing & Communication

- Use approved communication channels (company email, official messaging platforms, internal portals).
- Share information only with individuals who have a legitimate need to know.
- Do not disclose confidential or sensitive information without appropriate authorization.
- Maintain a log of critical communications and document distributions.

4.4 Confidentiality Protocols

- Encrypt sensitive digital records and communications.
- Mark confidential documents clearly with â€œConfidential.â€
- Shred or securely delete confidential materials when no longer needed.
- Report any breaches of confidentiality immediately to management.

4.5 Auditing

- Conduct regular audits (at least annually) of records, documentation, and communication practices.
- Document audit findings and take corrective actions for any deficiencies.
- Maintain audit reports for compliance verification.

5. Documentation & Record Retention Table

Document Type	Retention Period	Storage Location	Responsible Person
Personnel Records	7 years after separation	HR Secure Drive / Cabinet	HR Manager
Financial Records	7 years	Finance Secure Drive / Locked Office	Finance Officer
Confidential Reports	5 years or as required	Restricted Access Folder	Records Officer
Email Correspondence	2 years	Email Archive	IT Administrator

6. Compliance & Review

- All staff must be trained on this SOP.
- Non-compliance may result in disciplinary action.
- This SOP must be reviewed annually and updated as required.

7. Revision History

Version	Date	Description of Changes	Approved By
1.0	2024-06-15	Initial version	Head of Operations