# Standard Operating Procedure (SOP): Procedures for Document Sharing and Distribution

This SOP defines the **procedures for document sharing and distribution**, detailing standardized methods for securely sharing, distributing, and managing documents within the organization. It includes guidelines on document access permissions, version control, approved distribution channels, confidentiality considerations, and tracking mechanisms to ensure timely and efficient communication while maintaining data integrity and compliance with organizational policies.

## 1. Purpose

To establish standardized practices for the secure and efficient sharing and distribution of documents, ensuring data integrity, confidentiality, and compliance with regulatory and organizational requirements.

## 2. Scope

This SOP applies to all employees, contractors, and third-party vendors involved in the sharing or distribution of internal or external documents within the organization.

## 3. Responsibilities

- **Document Owner:** Initiates sharing/distribution and ensures compliance with this SOP.
- **IT Department:** Provides and maintains secure distribution platforms/tools.
- **Recipients:** Abide by confidentiality and security guidelines outlined for each document.
- **Compliance Officer:** Monitors adherence to policies and regulatory requirements.

## 4. Procedure

1. **Document Preparation**
   - Verify document completeness and accuracy.
   - Classify documents based on sensitivity and intended audience (e.g., Public, Internal, Confidential, Restricted).
   - Apply appropriate metadata (title, version, owner, date).
2. **Access Permission Management**
   - Set permissions according to document classification using access control lists (ACLs) on authorized platforms.
   - Restrict editing and sharing abilities to designated personnel only.
   - Review and update permissions periodically.
3. **Version Control**
   - Store documents in a centralized version-controlled repository (e.g., SharePoint, Google Drive, internal DMS).
   - Label each version clearly (e.g., v1.0, v1.1) and maintain a history of changes.
4. **Approved Distribution Channels**
   - Use only organization-approved channels: secure cloud platforms, encrypted emails, or internal DMS.
   - Prohibit use of unauthorized personal emails or external drives for distribution.
   - For external distribution, validate recipient identities and restrict access duration where possible.
5. **Confidentiality Considerations**
   - Mark confidential documents clearly (e.g., "CONFIDENTIAL" watermark).
   - Obtain signed NDAs where required before distribution.
   - Refrain from including sensitive data in the email body/text; share as secured attachments or links.
6. **Tracking & Acknowledgement**
   - Maintain distribution lists and logs for each document shared.
   - Require read receipts or acknowledgements for critical/confidential documents.
   - Regularly review distribution records and address any anomalies.
7. **Archiving & Retention**
   - Archive obsolete or superseded documents according to retention policy.
   - Restrict access to archived documents unless approved by management.

## 5. Compliance & Audit

- All document sharing and distribution activities are subject to regular audits.
- Non-compliance will result in corrective actions as per organizational policy.

## 6. References

- Document Management Policy
- Data Privacy and Protection Policy
- Acceptable Use Policy
- Relevant regulatory standards (e.g., GDPR, HIPAA, ISO/IEC 27001)

## 7. Review & Revision

- This SOP is to be reviewed annually or as required based on changes in regulations or organizational policy.
- Version history and changes must be documented in the SOP control log.

| SOP Owner | Approval Date | Next Review Date | Version |
|---|---|---|---|
| Document Control Manager | YYYY-MM-DD | YYYY-MM-DD | 1.0 |