

# Standard Operating Procedure (SOP): Document Distribution and Accessibility Protocols

This SOP defines the **document distribution and accessibility protocols**, detailing procedures for the secure and efficient dissemination of documents, ensuring authorized access, version control, and timely updates. It aims to maintain document integrity, confidentiality, and availability across the organization while supporting compliance with regulatory requirements and facilitating seamless communication among stakeholders.

## 1. Purpose

To outline standardized procedures for distributing organizational documents and managing their accessibility, ensuring secure, controlled, and compliant document handling.

## 2. Scope

This SOP applies to all employees, contractors, and stakeholders who create, manage, distribute, or access organizational documents in both physical and electronic formats.

## 3. Responsibilities

Role	Responsibility
Document Owner	Create, review, approve, and assign distribution lists.
Document Controller	Maintain version control, archive superseded documents, and monitor access logs.
IT/Admin	Maintain secure storage systems and manage user permissions.
All Users	Access and use documents per authorization, report discrepancies or unauthorized access.

## 4. Procedure

### 4.1 Document Classification

- Classify each document (e.g., Public, Internal, Confidential, Restricted).
- Label documents according to classification.

### 4.2 Document Distribution

- Send documents only to authorized personnel as per distribution list.
- Use approved distribution methods (e.g., secure email, document management system, physical handover with tracking).
- Ensure acknowledgment of receipt where required.

### 4.3 Accessibility Management

- Restrict document access based on user roles and authorization levels.
- Utilize document management tools with access controls and monitoring capabilities.
- Regularly review and update user permissions.

### 4.4 Version Control

- Assign version identifiers to each document update.
- Maintain a version history log including reasons for revision.
- Archive previous versions as per retention policy; only most recent version is for active distribution.

## 4.5 Document Updates

- Communicate all updates to relevant stakeholders promptly.
- Replace outdated versions in all repositories and remove from circulation.

## 4.6 Security & Confidentiality

- Encrypt confidential documents during transit and storage.
- Prohibit sharing of confidential documents through unsecured channels.
- Monitor and audit access logs for sensitive information.

# 5. Compliance and Monitoring

- Conduct periodic reviews to ensure compliance with regulatory requirements (e.g., GDPR, HIPAA).
- Regularly audit document access and distribution logs.
- Report and investigate breaches or non-compliance incidents.

## 6. Related Documents

- Document Retention Policy
- Data Privacy Policy
- Access Control Policy

## 7. Revision History

Version	Date	Description	Author
1.0	2024-06-08	Initial Release	[Your Name]