SOP Template: Guidelines for Document Transmission and Sharing

This SOP provides **guidelines for document transmission and sharing** to ensure secure, efficient, and consistent handling of documents across the organization. It covers protocols for choosing appropriate transmission methods, maintaining confidentiality and data integrity, adhering to compliance and legal requirements, managing access permissions, and tracking document sharing activities to prevent unauthorized access and data breaches.

1. Purpose

To establish standardized procedures for securely transmitting and sharing documents, safeguarding sensitive information, and ensuring regulatory compliance across the organization.

2. Scope

This SOP applies to all employees, contractors, and third parties involved in the transmission and sharing of organizational documents, whether in electronic or physical format.

3. Responsibilities

- **Document Owners**: Ensure documents are classified, transmitted, and shared according to this SOP.
- **Recipients**: Maintain the confidentiality and integrity of received documents.
- **IT Department**: Implement and manage secure transmission tools and protocols.
- **Compliance Team**: Monitor adherence and address any non-compliance issues.

4. Procedure

1. **Document Classification**
    - Classify documents based on sensitivity: Public, Internal, Confidential, or Restricted.
2. **Selection of Transmission Method**
    - Use approved methods (see Section 6) matching classification level.
    - High-sensitivity documents require secure, encrypted channels.
3. **Access Controls**
    - Share documents only with authorized personnel.
    - Use access permissions (e.g., view, edit, download) based on necessity.
4. **Confidentiality & Integrity**
    - Ensure encryption in transit and at rest for confidential/restricted documents.
    - Verify recipient identity before transmission.
5. **Compliance & Legal**
    - Comply with data protection regulations (GDPR, HIPAA, etc.).
    - Retain transmission logs as per legal requirements.
6. **Tracking & Auditing**
    - Maintain logs of all sharing activities for review and incident response.
7. **Incident Reporting**
    - Report accidental or unauthorized sharing immediately to the Compliance Team.

5. Transmission Methods

Method	When to Use	Security Features
Email (with encryption)	Internal/external sharing of medium-sensitivity documents	End-to-end encryption, password-protection, recipient verification

Secured File Sharing Platforms (e.g., SharePoint, OneDrive)	Internal collaboration and document workspace	Granular access controls, audit logging, encryption
Encrypted USB/Physical Delivery	When electronic transmission is not possible	Physical security, encrypted storage
Secure FTP/SFTP	Bulk file transfers between systems/locations	Encryption, access logging

6. Access Permission Management

- Assign document permissions based on the principle of least privilege.
- Review and update access permissions regularly.
- Revoke access promptly for terminated users or completed projects.

7. Tracking & Monitoring

- All transmissions and sharing actions must be logged automatically where possible.
- Conduct periodic audits of sharing activities.
- Flag and investigate unauthorized or unusual sharing behavior.

8. Training & Awareness

- Employees must undergo regular training on secure document transmission and sharing protocols.
- Provide updates as SOPs and legal requirements evolve.

9. Revision History

Date	Revision	Description
2024-06-01	1.0	Initial SOP created.