

SOP: Procedures for Sharing Confidential Information (Internal and External)

This SOP details **procedures for sharing confidential information** both internally within the organization and externally with authorized parties. It emphasizes the importance of maintaining data privacy and security by establishing protocols for information classification, authorized access, secure transmission methods, and verification processes. The document outlines steps to prevent unauthorized disclosure, ensure compliance with data protection regulations, and promote accountability among employees handling sensitive information. Implementing these procedures helps safeguard organizational integrity and protect confidential data from breaches or misuse.

1. Purpose

To define standardized procedures for sharing confidential information internally and externally, ensuring its protection and compliance with applicable regulations.

2. Scope

This SOP applies to all employees, contractors, and agents who handle confidential information in the course of their work with the organization.

3. Definitions

| Term | Definition |
|--------------------------|--|
| Confidential Information | Any non-public information that, if disclosed, could cause harm to the organization, its clients, or partners. |
| Internal Sharing | Disclosure or transmission of confidential information within the organization. |
| External Sharing | Disclosure or transmission of confidential information to individuals or entities outside the organization. |
| Authorized Access | Approval to view or handle confidential information, granted based on role or business need. |

4. Responsibilities

- **All Employees:** Adhere to this SOP when handling confidential information.
- **IT Department:** Ensure secure communication tools and monitor data transmission.
- **Managers/Supervisors:** Educate teams and monitor compliance.
- **Data Protection Officer:** Provide guidance, oversee compliance, and report incidents.

5. Procedures

5.1. Information Classification

1. Label all documents or data sets according to sensitivity (e.g., Public, Internal, Confidential, Restricted).
2. Review and update classification regularly.

5.2. Access Authorization

1. Grant access only to employees with a demonstrable business need.
2. Review and modify access rights periodically.

5.3. Internal Sharing Protocol

1. Verify recipient's authorization before sharing.
2. Use secure internal communication tools (e.g., encrypted email, authorized file-sharing platforms).
3. Never leave confidential information unattended or display on public screens.
4. Log and track access or transfers of highly sensitive data.

5.4. External Sharing Protocol

1. Verify that external parties are authorized according to signed NDAs or contracts.
2. Use approved secure transmission methods (e.g., end-to-end encrypted email, secure file transfer). Avoid public email and unapproved platforms.
3. Confirm the recipient's identity prior to sharing (e.g., phone verification, multi-factor authentication).
4. Share only the minimum necessary information.
5. Record all disclosures in the Information Sharing Log.

5.5. Secure Transmission Methods

- Use encryption for all confidential documents in transit and at rest.
- Password-protect files; communicate passwords through a separate secure channel.

5.6. Incident Reporting

1. Immediately report any suspected or actual unauthorized disclosure to the Data Protection Officer.
2. Participate in incident investigations and remediation procedures as required.

5.7. Compliance and Training

- Participate in mandatory annual training on data protection and confidentiality.
- Review and acknowledge updated SOPs and policies.

6. Records and Documentation

- Information Sharing Log (for all external disclosures)
- Access Authorization Records
- Incident Reports
- Training Attendance Logs

7. Review and Update

This SOP will be reviewed annually or when significant changes to relevant laws, regulations, or organizational operations occur.

8. References

- Data Protection Regulations (e.g., GDPR, CCPA)
- Company Information Security Policy
- Non-Disclosure Agreement (NDA) Templates