SOP: Confidential Information Handling and Sharing Rules

This SOP defines the **confidential information handling and sharing rules**, including guidelines for identifying confidential data, authorized access protocols, secure communication methods, data encryption standards, responsibilities for employees and third parties, procedures for sharing information internally and externally, handling data breaches, and compliance with legal and regulatory requirements. The objective is to protect sensitive information from unauthorized disclosure while ensuring it is shared appropriately to support business operations and maintain trust.

1. Purpose

To provide a standardized procedure for identifying, handling, and sharing confidential information to ensure security, legal compliance, and trust among stakeholders.

2. Scope

Applies to all employees, contractors, consultants, and authorized third parties who handle confidential information on behalf of the organization.

3. Definitions

- **Confidential Information:** Any data, document, or material classified by the organization as confidential, including but not limited to customer data, financial data, intellectual property, trade secrets, and employee records.
- **Authorized Personnel:** Individuals with official permission to access specific confidential information.
- **Data Breach:** Unauthorized access, use, disclosure, or loss of confidential information.

4. Identification of Confidential Information

- Label documents and communications containing confidential information as "Confidential."
- Maintain an inventory or registry of confidential data types and locations.
- Train staff on recognizing and classifying confidential information.

5. Authorized Access Protocols

- Access to confidential information is granted strictly on a need-to-know basis.
- Users must authenticate via strong passwords and/or multi-factor authentication.
- Review and revoke access regularly when roles change or upon termination.

6. Secure Communication Methods

- Use approved secure channels (e.g., encrypted email, secure file transfer services) for sharing confidential information.
- Prohibit disclosure of confidential information via unencrypted or unsecured platforms.
- Do not leave documents containing confidential information unattended in public or unprotected locations.

7. Data Encryption Standards

- Encrypt confidential data at rest and in transit using industry-approved standards (e.g., AES-256, TLS 1.2+).
- Regularly update and audit encryption tools and protocols.

8. Employee and Third-party Responsibilities

- Read, understand, and follow this SOP and related data protection policies.
- Sign confidentiality agreements where required.
- Immediately report any suspected or actual data breaches to IT/Security.
- Ensure third-party vendors comply with these standards as part of their contracts.

9. Procedures for Sharing Information

Internal Sharing

- Only share with authorized personnel as per role requirements.
- Validate recipient identity before sharing sensitive information.

External Sharing

- Seek approval from appropriate management or data owners prior to sharing confidential information externally.
- Use secure channels and ensure the recipient understands confidentiality requirements.
- Document and log all external data sharing instances.

10. Handling Data Breaches

1. Immediately report actual or suspected breaches to the IT/Security/Compliance department.
2. Contain the breach and mitigate risks as instructed by IT/Security.
3. Provide all necessary information for investigation and documentation.
4. Notify affected parties and regulators as required by law, following the organization's incident response plan.

11. Compliance and Legal Requirements

- Comply with all local, national, and international laws on data protection (e.g., GDPR, HIPAA, CCPA).
- Regularly review and update this SOP in accordance with changes to legal and regulatory requirements.
- Participate in mandatory training and awareness programs.

12. Document Control

Version	Date	Author	Description of Change
1.0	2024-06-01	Compliance Officer	Initial SOP Release