SOP: Secure Storage and Transportation of Sensitive Data

This SOP details the protocols for the **secure storage and transportation of sensitive data**, covering data encryption standards, access control measures, secure transfer methods, data integrity verification, compliance with privacy regulations, employee training on data handling, and incident response procedures. The objective is to protect sensitive information from unauthorized access, loss, or corruption during storage and transit, ensuring confidentiality, integrity, and availability at all times.

1. Scope

This SOP applies to all employees, contractors, and third parties handling sensitive data, including digital and physical formats, within the organization.

2. Definitions

Term	Definition
Sensitive Data	Information that if disclosed, accessed, or altered without authorization could result in harm to individuals or the organization (e.g., PII, PHI, financial data).
Encryption	The process of converting information into a secure format that prevents unauthorized access.
Access Control	Policies and mechanisms restricting access to data to authorized users only.

3. Responsibilities

- Managers: Ensure all staff are aware of and adhere to this SOP.
- IT Staff: Maintain encryption tools, access management, and conduct audits.
- All Employees: Follow protocols for storage, transfer, and reporting incidents.

4. Procedures

1. **Data Encryption Standards**
    - All sensitive data must be encrypted in transit and at rest using industry standards (e.g., AES-256, TLS 1.2+).
    - Encryption keys must be stored securely, with access restricted to authorized personnel only.
2. **Access Control Measures**
    - Implement role-based access control (RBAC).
    - Review access rights regularly and revoke access upon role changes or termination.
    - Use multi-factor authentication (MFA) for all systems storing or transferring sensitive data.
3. **Secure Transfer Methods**
    - Transfer data using encrypted channels (e.g., SFTP, HTTPS, VPN).
    - Physical media used for transportation must be encrypted and logged.
    - Transport physical media via trusted couriers; maintain chain-of-custody documentation.
4. **Data Integrity Verification**
    - Use checksums and cryptographic hash functions (e.g., SHA-256) to verify data integrity before and after transfer.
    - Log all verification outcomes and promptly address discrepancies.
5. **Compliance with Privacy Regulations**
    - Adhere to relevant laws and regulations (e.g., GDPR, HIPAA, CCPA).
    - Conduct regular compliance audits and update protocols as needed.
6. **Employee Training**
    - All staff must undergo annual data handling and security training.
    - Document completion and understanding of training modules.
7. **Incident Response Procedures**
    - Report any breach or suspected compromise immediately to the IT security team.
    - Secure and preserve evidence; contain the incident as per the organization's incident response plan.
    - Notify affected stakeholders and authorities in accordance with regulations.

5. Review and Update

This SOP shall be reviewed at least annually or upon significant changes to applicable regulations, technology, or organizational structure.

6. References

- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- California Consumer Privacy Act (CCPA)
- NIST SP 800-53: Security and Privacy Controls

7. Approval

Prepared By	Reviewed By	Approved By	Date
[Name]	[Name]	[Name]	[YYYY-MM-DD]