SOP: Secure Storage and Access Control of Records

This SOP defines the procedures for **secure storage and access control of records**, ensuring that all records are properly stored, protected from unauthorized access, and maintained in compliance with data protection policies. It covers secure physical and digital storage methods, access permissions, user authentication, regular audits, and protocols for record retrieval and disposal to maintain confidentiality, integrity, and availability of sensitive information.

1. Purpose

The purpose of this SOP is to establish standardized methods for securely storing, accessing, and managing records to protect sensitive information from unauthorized access, loss, or misuse.

2. Scope

This SOP applies to all personnel, contractors, and third parties who have access to company records, both physical and digital, including but not limited to documents, databases, and data storage devices.

3. Definitions

- **Records:** Any physical or digital documentation containing sensitive or proprietary information.
- **Access Control:** Processes that limit access to records based on user roles and authorization levels.
- **Authentication:** Verifying the identity of users attempting to access records.
- **Audit:** Regular review of access logs and storage protocols to ensure compliance.

4. Responsibilities

Role	Responsibility
Records Manager	Oversee and enforce storage and access control protocols, conduct audits.
IT Department	Implement and maintain secure digital storage systems and access controls.
All Staff	Comply with storage and access control procedures; promptly report any issues.

5. Procedures

5.1 Secure Physical Storage

- Store paper records in locked cabinets within secure areas accessible only to authorized personnel.
- Restrict physical access using keycards, locks, or other access control devices.
- Regularly review and update access lists for physical storage locations.

5.2 Secure Digital Storage

- Store digital records on encrypted servers with regular data backups.
- Use secure cloud storage providers compliant with relevant data protection regulations.
- Limit remote access to VPN-authenticated users only.

5.3 Access Permissions and User Authentication

- Grant access based on role and business necessity (principle of least privilege).
- Use strong, unique passwords and enable Multi-Factor Authentication (MFA) where possible.
- Disable accounts immediately upon staff departure or change in role.

5.4 Audits and Monitoring

- Perform quarterly audits of access logs and storage locations.
- Investigate and document any unauthorized access attempts.
- Update procedures based on audit findings and emerging threats.

5.5 Record Retrieval and Disposal

- Implement controlled check-out/check-in procedures for physical records.
- Ensure all retrieval requests are logged and authorized.
- Shred or securely wipe records scheduled for disposal; maintain a destruction log.

6. Compliance

All staff must follow this SOP and adhere to applicable regulations (e.g., GDPR, HIPAA). Violations may result in disciplinary action.

7. Review and Revision

This SOP shall be reviewed annually, or upon significant regulatory or organizational changes, to ensure continued effectiveness and compliance.

8. References

- Company Data Protection Policy
- Relevant Regulatory Requirements (e.g., GDPR, HIPAA)
- IT Security Standards