Standard Operating Procedure (SOP)
Access Control and Document Security Measures

Purpose

This SOP details **access control and document security measures** designed to protect sensitive information and restrict unauthorized access. It includes protocols for user authentication, physical and digital access restrictions, secure document storage, encryption practices, regular audits, and incident response plans. The objective is to ensure confidentiality, integrity, and availability of critical documents while minimizing risks of data breaches and unauthorized disclosures.

Scope

This SOP applies to all employees, contractors, and authorized users who access, manage, or store sensitive documents within the organization, whether in physical or electronic format.

Definitions

Term	Definition
Sensitive Information	Information that, if disclosed, could cause harm to the organization or individuals (e.g., personal data, financial records).
User Authentication	Process of verifying the identity of an individual requesting access to resources.
Encryption	Process of encoding data to prevent unauthorized access.

Procedures

1. **User Authentication and Access Control**
   - All users must be issued unique login credentials.
   - Passwords must meet complexity requirements and be changed regularly.
   - Multi-factor authentication (MFA) must be enabled for sensitive systems.
   - Access rights are granted based on role and reviewed quarterly.
2. **Physical Access Restrictions**
   - Secure areas must be protected by keycard or biometric access.
   - Visitors must be accompanied at all times and sign in/out.
   - Physical files must be stored in locked cabinets when not in use.
3. **Digital Document Security**
   - Files containing sensitive data must be stored on encrypted drives or document management systems with strict access permissions.
   - File transfers must use secure protocols (e.g., SFTP, HTTPS).
   - Cloud storage services must be approved by IT and use end-to-end encryption.
4. **Encryption Practices**
   - All sensitive documents must be encrypted at rest and in transit.

    - Encryption keys must be managed and stored securely, with access limited to authorized personnel.
5. **Regular Audits**
    - Conduct quarterly audits of access logs and permission settings.
    - Review security measures annually for effectiveness and compliance.
6. **Incident Response**
    - Immediately report suspected breaches or unauthorized access to the IT security team.
    - Follow the organization's incident response plan for containment, investigation, and remediation.
    - Maintain records of all incidents and corrective actions taken.

Responsibilities

- **Employees** â€“ Adhere to access policies, protect credentials, and promptly report suspicious activities.
- **IT Department** â€“ Implement and manage security controls, conduct audits, and oversee incident response.
- **Management** â€“ Ensure compliance, provide resources for training and enforcement, and regularly review policies.

References

- Information Security Policy
- Data Privacy Guidelines
- Incident Response Plan