SOP: Electronic Document Encryption and Password Protection Standards

1. Purpose

This SOP defines the **electronic document encryption and password protection standards** to safeguard sensitive information from unauthorized access. It includes guidelines for selecting strong encryption methods, implementing robust password policies, managing encryption keys securely, and ensuring compliance with data protection regulations. The purpose is to maintain the confidentiality, integrity, and availability of electronic documents by enforcing consistent and effective security measures.

2. Scope

This SOP applies to all employees, consultants, and authorized third parties who create, handle, store, transmit, or manage electronic documents containing sensitive or confidential information.

3. Definitions

Term	Definition
Encryption	The process of converting data into a coded format to prevent unauthorized access.
Password Protection	The use of passwords to restrict access to electronic documents or systems.
Encryption Key	A piece of information used to encrypt or decrypt data.
Sensitive Information	Any data classified as confidential, proprietary, or protected under regulations (e.g., personal data, financial records).

4. Standards

4.1 Encryption Requirements

- All sensitive electronic documents must be encrypted at rest and in transit.
- Use industry-standard encryption algorithms (e.g., `AES-256` or higher).
- Do not use outdated or weak encryption protocols (e.g., `DES` , `RC4`).

4.2 Password Protection

- All documents storing or transmitting sensitive data must be protected by a password.
- Passwords must meet the following criteria:
  - Minimum length: 12 characters
  - Must include uppercase, lowercase, numbers, and special characters
  - Should not contain dictionary words or personal information
- Password-protected archives (e.g., ZIP, PDF) must use strong encryption options where available.

4.3 Key and Password Management

- Encryption keys and passwords must be stored securely, never in plain text or unsecured locations.
- Use approved password managers or enterprise key management solutions.
- Rotate keys and passwords at least every 12 months or immediately if a compromise is suspected.
- Do not share passwords or encryption keys through unsecured channels (e.g., email, chat).

4.4 Regulatory Compliance

- Ensure encryption and password policies comply with relevant data protection regulations (e.g., GDPR, HIPAA, CCPA).
- Document and retain encryption method records for audit purposes.

5. Roles & Responsibilities

Role	Responsibility
All Personnel	Follow encryption and password protection policies; report any security incidents.
IT/Security Team	Implement and monitor encryption tools; provide training; manage encryption keys and password systems.
Managers/Supervisors	Ensure team compliance with this SOP.

6. Monitoring & Review

- Review and test encryption and password protection measures quarterly.
- Update this SOP regularly to reflect evolving security threats and regulatory requirements.

7. References

- NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices
- ISO/IEC 27001: Information Security Management Systems
- Company Data Security Policy

8. Revision History

Date	Version	Description of Change	Author
2024-06-10	1.0	Initial release	SOP Team