Standard Operating Procedure (SOP)
Encryption and Password Protection Measures

This SOP details **encryption and password protection measures** to safeguard sensitive data and ensure secure access control. It covers guidelines for creating strong passwords, utilizing encryption protocols for data storage and transmission, managing password policies and updates, implementing multi-factor authentication, and maintaining compliance with security standards. The goal is to protect information confidentiality, prevent unauthorized access, and enhance overall cybersecurity resilience.

1. Purpose

To establish consistent procedures for implementing encryption and password protection to secure data and systems against unauthorized access and cyber threats.

2. Scope

This SOP applies to all employees, contractors, and third parties who access, manage, or process sensitive information within the organization.

3. Responsibilities

- **IT Department:** Implement, monitor, and enforce encryption and password protection controls.
- **Managers:** Ensure team compliance with SOP requirements.
- **Employees/Users:** Adhere to password creation, management, and data encryption guidelines.

4. Procedures

4.1 Password Creation Guidelines

- Use a minimum of 12 characters.
- Include upper and lower case letters, numbers, and special characters.
- Avoid using easily guessed information (e.g., birthdays, common words).
- Do not reuse passwords across multiple accounts.

4.2 Password Management

- Change passwords at least every 90 days.
- Utilize organization-approved password managers for secure storage.
- Do not write down passwords or share them via insecure methods (e.g., email).
- Report suspected password compromise immediately to IT.

4.3 Encryption Protocols

- Apply AES-256 or higher encryption for data at rest and in transit.
- Utilize SSL/TLS protocols for secure web communications.
- Encrypt all portable storage devices before use.
- Ensure encryption keys are managed and stored securely.

4.4 Multi-Factor Authentication (MFA)

- Enable MFA on all systems and applications that support it.
- Authentication must require at least two of the following: something you know (password), something you have (token/device), or something you are (biometric data).

4.5 Password Policy and Updates

- Review and update password policies annually or when required by changes in security standards.
- Communicate changes in password requirements organization-wide.

4.6 Compliance and Monitoring

- Ensure all encryption and password protection measures comply with relevant industry/regulatory standards

(e.g., GDPR, HIPAA, ISO/IEC 27001).
- Conduct regular security audits and vulnerability assessments.
- Document incidents and report any non-compliance.

5. Training and Awareness

- Conduct annual cybersecurity training covering password and encryption best practices.
- Provide ongoing awareness updates for emerging threats and organizational policy changes.

6. Review and Revision

This SOP must be reviewed and updated annually or as significant changes in technology, business processes, or regulatory requirements occur.

7. References

- ISO/IEC 27001: Information Security Management
- GDPR (General Data Protection Regulation)
- HIPAA Security Rule

8. Approval

Prepared by: _____
Approved by: _____
Date: _____