INSERT LOGO

SECURITY OPERATING PROCEDURE

Procedure Name	Password Management

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Classification: Confidential

This document should be restricted to those with a specific need.

1. Purpose
The purpose of this procedure is to ensure the security of passwords used within [Your Organisation’s Name] by establishing guidelines for password creation, usage, and management to protect sensitive information and maintain compliance with security policies.

2. Scope
This procedure applies to all passwords used within [Your Organisation’s Name], including those for user accounts, system accounts, and administrative accounts.

3. Roles and Responsibilities

- **IT Administrator:** Responsible for implementing and enforcing password policies.
- **Users:** Responsible for creating and maintaining secure passwords.
- **Information Security Manager:** Responsible for reviewing and approving password management procedures and ensuring compliance.

4. Procedure

Step 1: Password Creation

- **Minimum Length:** Passwords must be at least 12 characters long.
- **Complexity Requirements:** Passwords must include a mix of uppercase and lowercase letters, numbers, and special characters.

- **Prohibited Elements:** Passwords must not contain easily guessable information such as usernames, birthdays, or common words.
- **Password Manager:** Users are encouraged to use an approved password manager to generate and store passwords securely.

Step 2: Password Usage

- **Confidentiality:** Users must keep their passwords confidential and not share them with anyone.
- **Unique Passwords:** Users must use unique passwords for different systems and applications.
- **Password Entry:** Users must ensure that no one can see their password when they enter it.

Step 3: Password Change

- **Regular Changes:** Passwords must be changed at least every 90 days.
- **Compromise Response:** If a password is suspected to be compromised, it must be changed immediately.
- **Notification:** Users will receive reminders to change their passwords before they expire.

Step 4: Password Recovery

- **Self-Service:** Users can use the self-service password recovery tool to reset their passwords.
- **Identity Verification:** Users must verify their identity through predefined security questions or multi-factor authentication before resetting their password.

5. Security Controls

- **Account Lockout:** Accounts will be locked after five consecutive failed login attempts.
- **Encryption:** Passwords must be stored using strong encryption methods.
- **Audit Logs:** Maintain logs of password changes and recovery activities.

6. Incident Management

- **Incident Identification:** Monitor for any unauthorized access attempts or suspicious activities related to password use.
- **Incident Response:** Report any incidents to the Information Security Manager immediately for investigation.
- **Incident Documentation:** Document the incident and the response actions taken.

7. Monitoring and Auditing

- **Policy Enforcement:** Regularly review and enforce compliance with password policies.
- **Periodic Audits:** Conduct periodic audits to ensure compliance with this procedure and identify any areas for improvement.

8. Review and Update

- **Review Frequency:** This procedure will be reviewed annually.
- **Update Process:** Any updates or changes to this procedure must be approved by the Information Security Manager.

9. References

- **Information Security Policy**
- **User Guide for Password Manager**
- **Password Recovery Tool User Guide**