Standard Operating Procedure (SOP)

Title: Secure Password Management

Document Version: 1.0
Effective Date: 08/08/2025
Prepared by: Semicolon

Approved by: Manager

Purpose

The purpose of this SOP is to define the process and best practices for creating, storing, updating, and managing passwords in a secure and efficient manner, ensuring protection against unauthorized access and data breaches.

Scope

This procedure applies to all users (employees, administrators, and external contractors) who access systems, applications, or platforms that require authentication via passwords.

Responsibilities

Users:

Create strong passwords, store them only within the password manager, and never share

credentials.

Administrators:

Maintain system security, ensure backups, and manage user access rights.

IT Security Team:

Monitor for suspicious activities, enforce password policies, and update security measures.

Procedure

User Registration

Users must register with verified email addresses and strong passwords.

Two-Factor Authentication (2FA) must be enabled.

Password Storage

All passwords are encrypted using AES-256 encryption.

Master passwords are never stored; they are hashed securely.

Password Retrieval

Users can retrieve stored passwords only after successful authentication and 2FA verification.

Backup & Recovery

Regular automated backups are stored in encrypted format.

Recovery keys are generated for emergency access.

Access Control

User roles define access levels (Admin/User/Read-Only).

Access logs are reviewed monthly for anomalies.

Security Measures

Enforce password complexity (minimum length, special characters, numbers).

Lock accounts after multiple failed login attempts.

Regular system penetration testing.

Review and Updates

This SOP will be reviewed every 6 months or when major security updates are made.