# Password Sharing Procedure

## 1. Introduction

This document outlines the Password Sharing Procedure for [Organization Name], ensuring compliance with ISO 27001 standards. It provides guidance on the controlled and secure handling of passwords to safeguard access to information systems and sensitive data.

## 2. Purpose

The purpose of this procedure is to prevent unauthorized access to information systems by eliminating unnecessary password sharing and ensuring that, when sharing is necessary, it is done securely and in accordance with organizational policies and regulatory requirements.

## 3. Scope

This procedure applies to all employees, contractors, and third parties with access to [Organization Name]'s systems and information. It covers all instances of password creation, sharing, and management within the organization.

## 4. Policy Statement

1. Password sharing is prohibited except in exceptional cases where operational requirements necessitate it, such as during critical system maintenance or emergency response activities. Authorization must be obtained from the system owner with documented justification.

2. Passwords must never be shared verbally, written in plain text, or transmitted via unsecured channels (e.g., email, instant messaging). Acceptable encrypted communication channels include end-to-end encrypted messaging applications such as Signal or encrypted email services.

3. Approved password-sharing methods include:

- Use of secure password management tools.

- Temporary sharing through encrypted communication channels.

4. Shared passwords must be changed within 15 minutes after their intended use to ensure consistent compliance and minimize risk.

5. All shared passwords must adhere to the organization’s password complexity and length requirements.

6. Any incident involving unauthorized password sharing must be reported to the Information Security Team immediately.

## 5. Roles and Responsibilities

- System Owners: Approve or deny password-sharing requests and ensure compliance with this procedure.

- Employees and Contractors: Adhere to password-sharing policies and report any incidents or violations.

- Information Security Team: Monitor compliance, provide guidance on secure sharing practices, and handle incident investigations.

- IT Department: Support secure password management tools and enforce technical controls for password sharing.

## 6. Compliance and Monitoring

Compliance with this procedure will be monitored through:  
- Regular audits of password-sharing practices.  
- Review of system access logs.  
- Incident reporting and investigation.  
Non-compliance will result in disciplinary actions, which may include training, access revocation, or other measures as deemed appropriate.

## 7. Related Documentation

- [Information Security Policy]

- [Access Control Policy]

- [Incident Management Procedure]

- [Password Management Policy]

## 8. Review and Revision

This procedure will be reviewed annually or whenever significant changes occur in organizational structure, technology, or regulatory requirements. The Information Security Team will initiate and document revisions as needed.

## Appendix A: Secure Password Sharing Guidelines

- Approved Methods:

- Secure password management tools.

- End-to-end encrypted communication channels (e.g., secure messaging applications).

- Prohibited Methods:

- Sharing via email, instant messaging, or unencrypted notes.

- Writing passwords on paper or in unsecured files.

## Appendix B: Incident Response for Password Sharing Violations

- Step 1: Report the incident to the Information Security Team immediately.

- Step 2: The Information Security Team will investigate the scope and impact of the violation.

- Step 3: Affected accounts must have their passwords changed immediately.

- Step 4: Root cause analysis will be conducted, and corrective actions will be implemented.

- Step 5: A report will be prepared and shared with relevant stakeholders.