Popular Vehicles & Services

Policy Related to Information Technology Security

PASSWORD & AUTHENTICATION POLICY

Document Title : Password & Authentication Policy

Version : 1.0

Effective Date : 31-01-2026

Review Cycle : Annual

Policy Owner : IT / Information Security

Approval Authority : Management / Board of Directors

---

1. Purpose

The purpose of this policy is to define password and authentication requirements that protect organizational information systems from unauthorized access. This policy establishes consistent authentication standards, strengthens access security, and supports compliance with Information Security governance and Information Systems audit requirements.

---

2. Scope

This policy applies to all employees, contractors, consultants, and authorized third parties who access organizational information systems. It covers all systems, applications, infrastructure, cloud services, and authentication mechanisms, including on-premises, remote, and cloud-based access.

---

3. Authentication Principles

The organization shall:

Enforce strong and consistent authentication mechanisms to protect systems, applications, and data

Apply additional authentication controls for privileged, remote, and high-risk access

Prevent unauthorized access through account lockout and monitoring controls

Ensure authentication credentials are protected against misuse, disclosure, or compromise

---

4. Roles and Responsibilities

Management / Business Owners:

- Ensure compliance with this policy within their teams
- Support enforcement of authentication and access controls

IT / Information Security:

- Configure, implement, and enforce password, MFA, and account lockout controls
- Monitor authentication-related security events and access attempts
- Maintain configuration records and audit evidence to demonstrate compliance

Users:

- Protect passwords and authentication factors from unauthorized use
- Not share credentials with others under any circumstances
- Promptly report suspected or actual credential compromise or misuse

---

5. Policy Statements

Password Complexity and Length:

- Passwords shall have a minimum length of 12 characters
- Passwords shall include a combination of uppercase letters, lowercase letters, numbers, and special characters
- Use of default, weak, or commonly used passwords is prohibited

Password Management:

- Passwords shall not be reused across organizational systems
- Passwords shall not be written down, shared, or stored in plain text
- Passwords shall be changed immediately if compromise is suspected

Multi-Factor Authentication (MFA):

Multi-factor authentication (MFA) shall be enforced for:

- Administrative and privileged accounts
- Remote access such as VPN
- Cloud platforms and services
- Corporate email systems

MFA mechanisms shall be approved and managed by IT / Information Security

Account Lockout:

- User accounts shall be locked after a defined number of unsuccessful authentication attempts
- Account lockout settings shall be configured to reduce the risk of brute-force and password-guessing attacks
- Locked accounts shall be unlocked only through authorized processes

Credential Storage:

- Passwords and authentication credentials shall be **stored securely** using approved encryption or hashing mechanisms
- Storage of credentials in clear text, scripts, or unsecured files is strictly prohibited
- System-generated or temporary credentials shall be changed upon first use

---

6. Audit and Evidence

The following audit evidence shall be maintained and made available upon request:

- Password policy configuration settings
- MFA enforcement records or screenshots
- Account lockout configuration details
- Authentication and access logs for critical systems

---

7. Compliance

Compliance with this policy is mandatory. Non-compliance may result in disciplinary action in accordance with organizational policies and applicable laws. Approved exceptions shall be formally documented.

---

8. Review

This policy shall be reviewed annually or upon significant changes to systems, authentication mechanisms, or regulatory requirements.

---

9. Approval

This policy has been reviewed and approved by the following authorities:

Role	Name	Signature	Date
Board of Directors / Management.			
Head – IT			