Password Policy

1. Purpose / Objective

The purpose of this policy is to define requirements for creating, using, and protecting passwords that safeguard access to company systems, applications, and data. Strong password practices reduce the risk of unauthorized access and protect the confidentiality, integrity, and availability of company information.

---

2. Scope

This policy applies to:

- All employees, contractors, interns, and third parties with access to company IT systems.
- All systems, applications, and services that require authentication, whether cloud-based or on-premises.

---

3. Policy Statement

- Passwords **must** be at least 12 characters long and include a mix of uppercase, lowercase, numbers, and special characters.
- Passwords **must not** contain easily guessable words (e.g., company name, “password123”, birth dates).
- Multi-Factor Authentication (MFA) **must** be enabled where supported.
- Passwords **must** be changed at least every 90 days, or immediately if compromise is suspected.
- The reuse of the last 5 passwords is prohibited.
- Passwords **must not** be shared, written down, or stored in plain text.
- Accounts will be locked after 5 failed login attempts and can only be reset through the IT Security Department.
- Default vendor/system passwords **must** be changed before use.

---

4. Roles & Responsibilities

- **Employees / Users**: Responsible for creating and safeguarding strong passwords, reporting suspected compromise immediately.

- **IT Security Department**: Enforce technical password controls (complexity rules, expiry, lockout), monitor suspicious activity, and provide secure password reset mechanisms.
- **Management**: Ensure staff are trained and aware of password requirements.

---

5. Compliance & Enforcement

- Non-compliance may result in:
    - Revocation of system access.
    - Disciplinary action, up to termination of employment.
    - Legal action in case of deliberate compromise.

---

6. References

- ISO/IEC 27001: Annex A.5.17 – Authentication Information
- NIST SP 800-63B – Digital Identity Guidelines
