Password Policy & Compliance Checklist

(Aligned with ISO/IEC 27001, SOC 2, and NIST SP 800-63B)

Prepared by…..

Mizanur Rahman Pranto

LinkedIn | Email

All images and illustrations were created using AI tools.

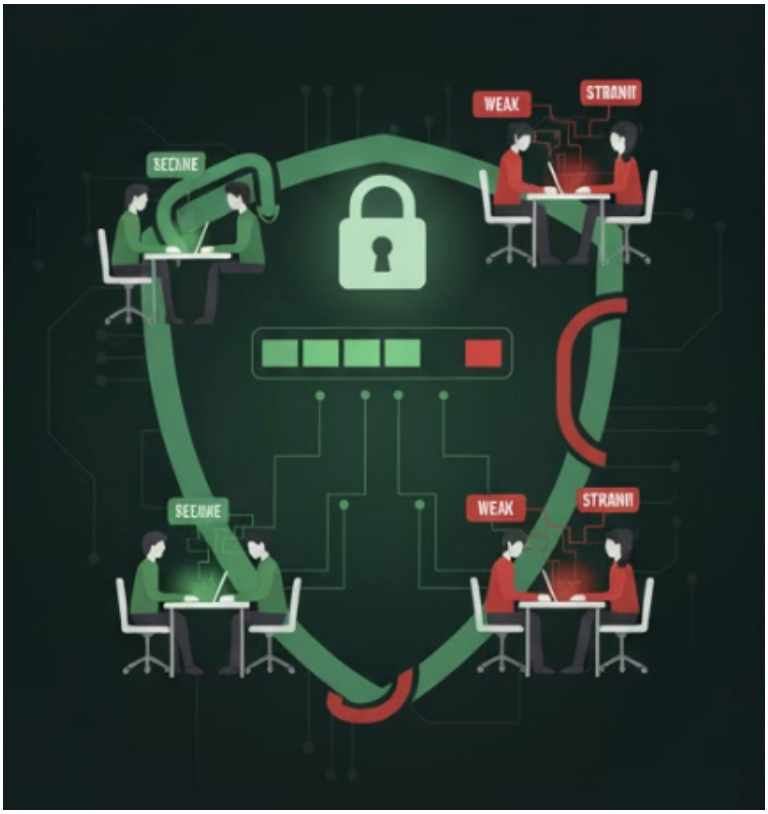
Table of Contents

PASSWORD POLICY

(Aligned with ISO/IEC 27001 : 2022 Controls A.5.15, A.5.17 | SOC 2 CC6.1 – CC6.2 | NIST SP 800-63B)

1. Purpose

This policy establishes standardized controls for password creation, protection, and management to safeguard organizational systems and data against unauthorized access.
It aligns with **ISO 27001**, **SOC 2**, and **NIST** password security requirements to ensure confidentiality, integrity, and availability of information assets.



2. Scope

This policy applies to:

- All employees, contractors, vendors, and third-party users.
- All information systems, applications, servers, databases, and network devices owned or managed by the organization.
- Both on-premises and cloud environments requiring user authentication.

3. Objectives

- To define strong password standards compliant with international frameworks.
- To protect credentials against unauthorized disclosure or misuse.
- To enforce consistent authentication mechanisms across all systems.

4. Policy Statement

The organization mandates the use of strong, unique passwords or passphrases for every system account.
Passwords must be managed and stored securely, protected through encryption, and supported by multi-factor authentication (MFA) for critical systems.

5. Roles and Responsibilities

5.1 Information Security Team

- Define and maintain password management standards.
- Monitor compliance and perform regular audits.
- Ensure password storage systems use approved cryptographic algorithms.

5.2 System Administrators

- Enforce password complexity and MFA on all systems.
- Disable or change default credentials before system deployment.
- Maintain logs of password-related security events.

5.3 Employees and Contractors

- Comply with password requirements and protect credentials.
- Report suspected password compromise immediately.

6. Password Requirements

6.1 Password Length and Complexity

- Minimum length: **12 characters** (recommended 14+ for admins).
- Must contain **uppercase**, **lowercase**, **number**, and **special character**.
- Passphrases encouraged (e.g., “RedCar!Drives2025”).

6.2 Password History and Reuse

- Users cannot reuse their **last 5 passwords**.
- Passwords exposed in known data breaches are strictly prohibited (checked via breach databases).

6.3 Password Expiration and Rotation

- No periodic expiration without cause, following **NIST SP 800-63B**.
- Change passwords immediately after compromise or role change.
- Privileged account passwords rotated every **180 days**.

6.4 Prohibited Passwords and Patterns

- Do not use company name, username, “password123”, or dictionary words.
- Avoid sequential or repetitive characters (e.g., “1111”, “abcd”).

6.5 Passphrase Guidelines

- Use multiple random words separated by special characters.
- Minimum length 16 characters.
- Easier to remember yet strong against brute-force attacks.

7. Password Protection

7.1 Storage and Encryption

- Store passwords using strong **salted one-way hashes** (e.g., bcrypt, Argon2, PBKDF2).
- Plaintext storage strictly prohibited.

7.2 Transmission Security

- Always transmit passwords over **encrypted channels (TLS 1.2 or higher)**.
- Never share passwords through email or instant messaging.

7.3 Password Manager Usage

- Only approved corporate password managers may be used.
- Passwords stored locally must be encrypted and protected with MFA.

7.4 Handling Default Credentials

- Change or disable vendor-supplied default passwords before deployment.
- Verify all default accounts during system hardening.

8. Authentication Controls

8.1 Multi-Factor Authentication (MFA)

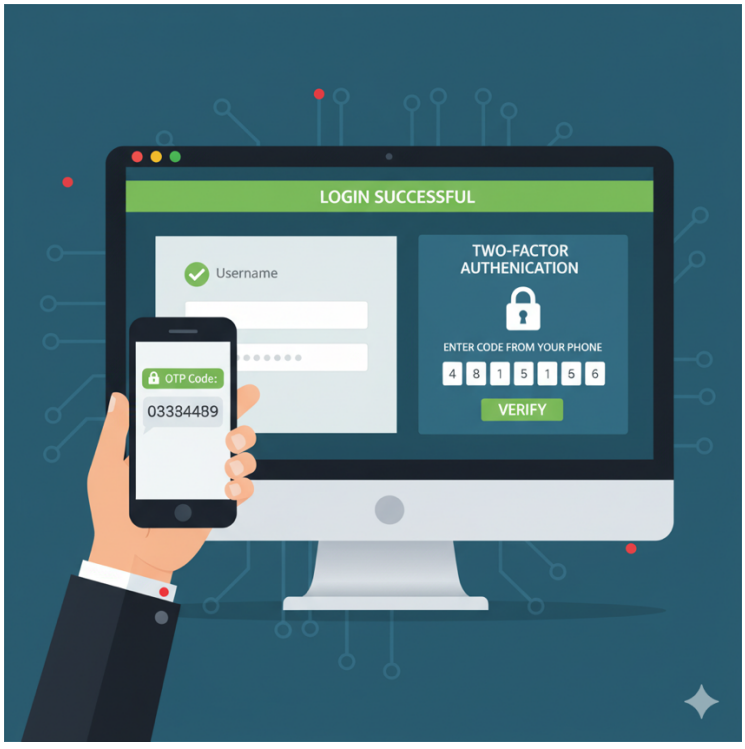
- MFA required for all:
  - Remote access (VPN, cloud, web portals)
  - Administrative and privileged accounts
  - Access to sensitive data or systems

8.2 Account Lockout Threshold

- Lock account after **5 failed login attempts**.
- Auto-unlock after **15 minutes** or upon admin approval.

8.3 Session Timeout and Reauthentication

- Idle sessions expire after **15 minutes** of inactivity.
- Reauthentication required for high-risk operations.



9. Administrative Accounts and Privileged Access

9.1 Privileged Account Rotation

- Rotate passwords at least every **180 days**.
- Use automated **Privileged Access Management (PAM)** tools.

9.2 Shared Account Prohibition

- Shared passwords are prohibited.
- Each privileged user must have a distinct account.

9.3 Privileged Access Management (PAM)

- PAM solutions must log credential use and provide access reviews.

10. Monitoring and Auditing

10.1 Logging of Authentication Events

- Record all successful and failed authentication attempts.
- Logs must be time-synchronized and protected against alteration.

10.2 Regular Compliance Review

- Conduct quarterly password audits.
- Verify compliance with ISO, SOC 2, and NIST standards.

10.3 Reporting and Incident Response

- Report password compromise immediately to the SOC or Security Team.
- Reset affected passwords and investigate any related security events.

11. User Responsibilities

- Never share, write down, or reuse passwords.
- Report any phishing or credential compromise attempts.
- Use different passwords for personal and business systems.
- Participate in cybersecurity awareness training.

12. Policy Enforcement

Non-compliance may lead to disciplinary action, access revocation, or termination. Repeated violations may be escalated to management or HR depending on severity.

13. Exceptions

Any deviation from this policy must be formally approved by the **Information Security Manager** and documented with mitigation controls.

14. References and Standards

- **ISO/IEC 27001:2022** — A.5.15 Access Control, A.5.17 Authentication Information, A.8.9 Configuration Management
- **SOC 2 Trust Services Criteria** — CC6.1, CC6.2
- **NIST SP 800-63B** — Digital Identity Guidelines (Authenticator & Verifier Requirements)

15. Revision History

Version	Date	Description	Author	Approved By
1.0	Oct 2025	Initial release	Information Security Team	CISO

PASSWORD POLICY COMPLIANCE CHECKLIST

(ISO 27001, SOC 2, NIST SP 800-63B Aligned)

Table Format

Requirement	Control Description	Responsible Party	Frequency	Compliance Status (Yes/No)	Evidence/ Remarks

1. General Controls

	Requirement	Control Description	Responsible Party	Frequency	Compliance Status	Evidence/ Remarks
1	Password policy formally documented	Verify that a written password policy exists, approved by management.	Information Security Manager	Annual		
2	Policy reviewed periodically	Review policy every 12 months or after major security events.	ISMS Officer	Annual		
3	Policy aligned with ISO 27001, SOC 2, NIST	Ensure cross-mapping of controls with international standards.	Compliance Officer	Annual		

2. Password Creation & Complexity Requirements

	Requirement	Control Description	Responsible Party	Frequency	Compliance Status	Evidence/ Remarks
1	Minimum length (≥12 characters)	Validate password policy configuration in AD, IAM, or SSO.	System Administrator	Quarterly		
2	Complexity enforced	Check use of uppercase, lowercase, numeric, and special characters.	IT Security	Quarterly		
3	Passphrase supported	Ensure users can use passphrases (e.g., longer phrases).	IT Security	Annually		
4	Breach database check	Passwords must be screened against known compromised passwords.	SOC / IT Security	Quarterly		
5	Password reuse restriction	Ensure at least last 5 passwords are not reusable.	IT / IAM	Quarterly		

3. Password Storage & Protection

	Requirement	Control Description	Responsible Party	Frequency	Compliance Status	Evidence/ Remarks
1	Passwords hashed with strong algorithm	Verify bcrypt/Argon2/PBKDF2 hashing used in systems.	System Admin	Quarterly		
2	Salt used for each password	Confirm that unique salts are applied per password.	Security Engineer	Annual		
3	Plaintext passwords prohibited	Audit systems for plaintext or reversible encryption.	SOC Team	Quarterly		
4	Secure transmission	Verify password transmission uses TLS 1.2+ or SSH.	Network Admin	Quarterly		

4. Authentication & Access Control

	Requirement	Control Description	Responsible Party	Frequency	Compliance Status	Evidence/ Remarks
1	Multi-Factor Authentication (MFA)	Confirm MFA implemented for privileged and remote accounts.	IT Security	Quarterly		
2	Account lockout policy	Lock account after 5 failed login attempts.	IT Administrator	Quarterly		
3	Session timeout	Idle sessions auto-logout after 15 minutes.	System Admin	Quarterly		
4	Default passwords removed	All default vendor passwords must be changed pre-deployment.	DevOps / IT	Per deployment		

5. Privileged Account Management

	Requirement	Control Description	Responsible Party	Frequency	Compliance Status	Evidence/ Remarks
1	Privileged password rotation	Rotate admin passwords every 180 days.	IT Admin	Semiannual		
2	PAM tool in use	Verify usage of Privileged Access Management (PAM) solution.	IT Security	Annual		
3	No shared accounts	Confirm all privileged accounts are unique and traceable.	Security Manager	Quarterly		

6. Monitoring & Logging

	Requirement	Control Description	Responsible Party	Frequency	Compliance Status	Evidence/ Remarks
1	Log authentication events	All login success/fail events logged.	SOC Team	Continuous		
2	Audit password changes	Password change events logged and reviewed.	SOC / ISMS	Monthly		
3	Review access logs	Verify logs reviewed periodically for anomalies.	SOC Analyst	Monthly		

7. User Training & Awareness

	Requirement	Control Description	Responsible Party	Frequency	Compliance Status	Evidence/ Remarks
1	Awareness training provided	Conduct annual password and MFA training.	HR / Security Awareness Team	Annual		
2	Phishing simulation awareness	Include credential protection in phishing simulations.	SOC / HR	Semiannual		
3	Users report compromises	Ensure reporting procedure for suspected password leaks.	All Employees	Ongoing		

8. Policy Review & Updates

	Requirement	Control Description	Responsible Party	Frequency	Compliance Status	Evidence/ Remarks
1	Annual review	Conduct a formal review of the password policy.	ISMS Officer	Annual		
2	Policy approval	Ensure CISO or top management approval for updates.	Compliance Officer	Annual		
3	Update based on incidents	Update policy after password-related incidents or audits.	Security Team	As needed		

Notes for Use

- **“Responsible Party”** can be customized per department (e.g., SOC, IT Admin, CISO).
- **“Evidence/Remarks”** may include screenshots, system configs, or audit reports.
- This table can be used directly in Excel, Notion, or an ISO 27001 ISMS tracking system.