Prompt: Generate a Secure password policy. Ensure security best practices.

**Password Policy**  
**Effective Date:** [Insert Date]  
**Last Updated:** [Insert Date]  
**Applicable To:** All employees, contractors, vendors, and third parties with access to [Company Name] systems, data, or applications.

**1. Purpose**

This policy defines requirements for creating, managing, and securing passwords to protect [Company Name]’s systems, networks, and data from unauthorized access, breaches, or misuse.

**2. Scope**

Applies to all passwords used to access:

* Workstations, servers, and databases
* Email, cloud services, and SaaS applications
* VPNs, remote access tools, and internal networks
* Mobile devices and privileged accounts (e.g., admin, root)

**3. Password Requirements**

**3.1 Password Creation**

All passwords **MUST**:

* Be a **minimum of 12 characters** (15+ for privileged/administrative accounts).
* Include **3 of the following**: uppercase letters, lowercase letters, numbers, and special symbols (e.g., !@#$%^&\*).
* **Avoid**:
  + Common phrases (e.g., "Password123"), company names, or personal information (e.g., birthdays).
  + Sequential/repeating characters (e.g., "12345", "aaaaa").
* Use **passphrases** where possible (e.g., "PurpleTiger$RunsFast!2024").

**3.2 Password Expiration**

* **Standard users**: Change passwords every **90 days**.
* **Privileged/administrative accounts**: Change every **60 days**.
* **Immediate reset** if a breach is suspected.

**3.3 Password Reuse**

* **Do NOT reuse** the last **5 passwords**.
* **Do NOT use the same password** across multiple systems (e.g., corporate vs. personal accounts).

**3.4 Multi-Factor Authentication (MFA)**

* **MFA is mandatory** for:
  + Remote access (VPN, cloud services).
  + Privileged accounts and sensitive systems (e.g., financial databases).
  + All users handling confidential data.

**4. Account Protection**

* **Account Lockout**: Accounts lock after **5 failed login attempts** (30-minute lockout period).
* **Session Timeout**: Inactivity sessions terminate after **15 minutes**.
* **Password Sharing**: Never share passwords via email, chat, or unsecured channels. Use a company-approved password manager for secure sharing.

**5. Storage & Transmission**

* **Never store passwords** in plain text (e.g., spreadsheets, sticky notes).
* Use **approved password managers** (e.g., LastPass, 1Password) for storage.
* Transmit passwords only via encrypted channels (e.g., HTTPS, TLS).

**6. Training & Awareness**

* **Annual training** on password security, phishing, and social engineering.
* **Report suspected compromises** immediately to IT/security teams.

**7. Enforcement**

* **Non-compliance** may result in revoked access, disciplinary action, or termination.
* IT will **audit password practices** quarterly and enforce policy updates.

**8. Exceptions**

* Temporary exemptions require written approval from the **CISO or IT Director**.

**Policy Owner:** [IT Security Team/CISO Name]  
**Review Cycle:** Annual or after significant security incidents.

*[Company Name] reserves the right to update this policy to align with evolving threats and industry standards (e.g., NIST, ISO 27001).*

**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**[Authorized Executive Name/Title]**  
**[Date]**