Prompt: Generate a policy for password policy.

Here’s a expanded password policy tailored to modern security standards, incorporating best practices and clarity:

**Password Security Policy**

**1. Purpose**

This policy ensures the creation, management, and protection of strong passwords to safeguard organizational systems, data, and user accounts against unauthorized access, breaches, and cyber threats.

**2. Scope**

Applies to all individuals with access to company resources, including:

* Employees (full-time, part-time, temporary)
* Contractors, vendors, and third-party partners
* Service accounts and system administrators

**3. Password Requirements**

**3.1 General Standards**

* **Minimum Length**: 12 characters.
* **Complexity**: Must include **three of the following**:
  + Uppercase letters (A-Z)
  + Lowercase letters (a-z)
  + Numbers (0-9)
  + Special characters (e.g., ! @ # $ % ^ & \*)
* **Prohibited Patterns**:
  + No sequential/repeating characters (e.g., 12345, aaaaa).
  + No personal information (e.g., names, birthdates, company name).
  + No common passwords (e.g., Password123!, Welcome1).

**3.2 Password Expiration & Reuse**

* **Expiration**: Passwords must be changed every **60 days**.
* **Reuse Prevention**: Users cannot reuse any of their **last 8 passwords**.

**3.3 Account Lockout & Monitoring**

* **Lockout Threshold**: Accounts lock after **5 consecutive failed attempts**.
* **Lockout Duration**: 15 minutes (auto-unlock).
* **Suspicious Activity**: Repeated failed logins trigger an alert to the IT Security team.

**4. Multi-Factor Authentication (MFA)**

* **Mandatory MFA**: Required for:
  + All remote/virtual private network (VPN) access.
  + Administrative/privileged accounts.
  + Access to sensitive systems (e.g., financial, HR, customer data).
* **MFA Methods**: Use authenticator apps (e.g., Google Authenticator, Microsoft Authenticator) or hardware tokens. SMS-based codes are discouraged.

**5. Secure Password Practices**

**5.1 Storage & Sharing**

* **Do NOT**:
  + Write down passwords on paper, sticky notes, or unsecured files.
  + Share passwords via email, chat, or phone.
* **Secure Sharing**: Use **IT-approved password managers** (e.g., Bitwarden, Keeper) for sharing credentials internally.

**5.2 Password Managers**

* **Mandatory Use**: Required for storing and generating passwords for business accounts.
* **Approved Tools**: IT will provide a company-managed password manager.

**6. Prohibited Practices**

* **Password Sharing**: Never share personal or shared account credentials unless authorized.
* **Default Passwords**: Change default passwords on devices/software immediately after setup.
* **Auto-Save**: Disable browser/application password auto-save features.

**7. Incident Response**

* **Compromised Passwords**: Report suspected breaches immediately to IT Security.
  + Change the password and log out of all active sessions.
* **Phishing Awareness**: Forward suspicious emails to the security team; do not enter passwords on untrusted sites.

**8. Training & Awareness**

* **Annual Training**: All users must complete cybersecurity training covering password hygiene.
* **Simulated Phishing Tests**: Conducted quarterly to reinforce vigilance.

**9. Enforcement**

* **Non-Compliance**: May result in:
  + Temporary loss of system access.
  + Disciplinary action, up to termination.
  + Legal consequences for negligence leading to breaches.

**10. Exceptions**

* **Service Accounts**: Must use machine-generated passwords (25+ characters) stored in a secure vault.
* **Legacy Systems**: Exemptions require written approval from IT Security.

**11. Review & Updates**

* Reviewed **every 6 months** or after major security incidents.
* Updates communicated via email and the company intranet.

**Effective Date**: [Insert Date]  
**Approved By**: [CISO/IT Director Name]