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

**[Your Company Name] Password Policy**

Effective Date: [Date]

Last Reviewed: [Date]

1. Purpose

This policy establishes the requirements for creating, managing, and securing passwords for all [Your Company Name] information systems and data. Adherence to this policy is crucial for protecting the confidentiality, integrity, and availability of our company's assets and information. This policy is designed to reflect current cybersecurity best practices, including guidelines from the National Institute of Standards and Technology (NIST) and other leading security organizations.

2. Scope

This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing [Your Company Name]'s internal networks, systems, applications, and data, whether on-site or remotely.

3. Policy Statements

3.1. Password Creation and Construction

* Minimum Length: Passwords must have a minimum length of 12 characters. For privileged accounts (e.g., administrator, system, service accounts), a minimum length of 15 characters is required.
* Complexity is Encouraged, Length is Prioritized: While complex combinations of character types (uppercase, lowercase, numbers, symbols) are encouraged, the primary focus is on password length. Longer passphrases are generally stronger than shorter, more complex ones.
* Character Set: Passwords must allow the use of all printable ASCII characters, including spaces, and Unicode characters (e.g., emojis, international characters).
* Uniqueness:
  + Passwords must be unique and not reused across different [Your Company Name] accounts.
  + Passwords must not be reused across work and personal accounts.
  + Passwords must be significantly different from previously used passwords (e.g., a history of at least 5 previous passwords will be maintained and reuse prevented).
* Prohibited Passwords:
  + Passwords must not be based on easily guessable information, such as:
    - Usernames, login IDs, or derivatives thereof.
    - Family names, pet names, birthdays, addresses, phone numbers.
    - Company name, common terms related to the company or industry.
    - Sequential characters (e.g., "123456", "abcdef").
    - Repetitive characters (e.g., "aaaaaa", "111111").
    - Common dictionary words or keyboard patterns (e.g., "password", "qwerty").
  + Passwords will be screened against a database of known compromised passwords. If a chosen password is found in this database, it will be rejected, and the user will be required to select a different password.

3.2. Password Protection and Handling

* Confidentiality: Users are responsible for maintaining the confidentiality of their passwords.
  + Passwords must not be written down and left in unsecured locations (e.g., sticky notes, under keyboards).
  + Passwords must not be shared with anyone, including colleagues, supervisors, or IT support staff. IT staff will never ask for your password.
  + Passwords must not be transmitted via unsecured electronic communication channels (e.g., email, instant messaging).
* Password Managers: The use of company-approved password managers is strongly encouraged to generate, store, and manage strong, unique passwords securely. Users should secure their master password for the password manager with the same rigor as any other critical password.
* Browser Storage: Storing passwords in web browsers is discouraged. If used, the browser's master password feature (if available and strong) must be enabled.
* Secure Storage (System Level): All system-stored passwords must be protected using strong, industry-standard cryptographic hashing and salting mechanisms (e.g., Argon2, scrypt, bcrypt, PBKDF2).

3.3. Password Changes

* Compromise-Driven Changes: Users must change their password immediately if they suspect it has been compromised or if notified by IT/Security personnel of a potential compromise.
* No Mandatory Periodic Expiration (for most user accounts): Regular, forced password expiration for standard user accounts is not required unless there is evidence of compromise or specific regulatory/compliance requirements dictate otherwise. This approach aims to encourage the creation of stronger, more memorable passphrases rather than predictable, incremental changes.
* Privileged Account Password Rotation: Passwords for privileged accounts may be subject to more frequent rotation (e.g., annually or semi-annually) or upon changes in personnel with access to these accounts, as determined by the IT/Security department.
* First-Time Use: Default or temporary passwords must be changed upon first login.

3.4. Multi-Factor Authentication (MFA)

* MFA Requirement: Multi-Factor Authentication (MFA) must be enabled and used for all accounts where it is available, especially for:
  + Remote access to [Your Company Name] networks and systems.
  + Access to sensitive data or critical systems.
  + All privileged accounts.
* Approved MFA Methods: Only company-approved MFA methods (e.g., authenticator apps, hardware tokens, biometrics) should be used. SMS-based MFA should be avoided where stronger alternatives are available due to known vulnerabilities.

3.5. Account Lockout

* Failed Login Attempts: Accounts will be temporarily locked out after a specified number of consecutive unsuccessful login attempts (e.g., 5-10 attempts).
* Lockout Duration: The lockout duration will be set to a reasonable period (e.g., 15-30 minutes) or require administrator intervention for persistent lockouts.
* Notification: Users should be notified (where feasible and secure) of account lockout events.

3.6. Password Recovery

* Secure mechanisms will be provided for password recovery.
* Knowledge-Based Authentication (KBA) or "security questions" with easily discoverable answers (e.g., "mother's maiden name," "first pet's name") should not be the sole method for account recovery.
* Password hints are prohibited.

3.7. User Responsibilities

* All users are responsible for familiarizing themselves with and adhering to this policy.
* Users must promptly report any suspected password compromise or security incident to the IT/Security department.
* Users are encouraged to use strong, unique passphrases and practice good password hygiene.

3.8. Shared and Service Accounts

* Shared accounts are generally discouraged. Where necessary for business operations, they must be approved by management and have their passwords managed securely and changed regularly, especially when an individual with access leaves the team or company.
* Service account passwords must be strong, unique, and managed securely. They should be changed periodically or when the system configuration changes.

4. Policy Enforcement

* Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract,1 and potential legal action in accordance with applicable laws and company policies.
* Technical enforcement controls will be implemented where possible to ensure compliance (e.g., minimum password length, history, lockout).

5. User Education and Training

* [Your Company Name] will provide regular security awareness training, including guidance on creating strong passwords, recognizing phishing attempts, and other password security best practices.

6. Policy Review and Updates

* This policy will be reviewed and updated annually, or as needed, to reflect changes in technology, threat landscape, business requirements, and cybersecurity best practices.

7. Exceptions

* Any exceptions to this policy must be documented, justified, and approved in writing by the Head of IT/Security or an authorized delegate. Approved exceptions will be reviewed periodically.

8. Contact

For any questions or clarifications regarding this policy, please contact the IT/Security Department at [IT/Security Department Contact Information].

Acknowledgment

I, [Employee/User Name], acknowledge that I have read, understood, and agree to comply with the [Your Company Name] Password Policy.

Signature Date