Prompt: Generate a policy for password policy.

**[Your Company Name] Password Policy**

Effective Date: [Date]

Last Reviewed: [Date]

1. Purpose

This policy outlines the requirements for creating and managing passwords to protect [Your Company Name]'s information assets, systems, and accounts from unauthorized access. Adherence to this policy is mandatory for all employees, contractors, and any other individuals with access to company systems and data.

2. Scope

This policy applies to all passwords used to access [Your Company Name] networks, applications, databases, and any other systems or services, whether company-owned or third-party services used for company business.

3. Policy Statements

3.1. Password Creation & Strength

* Minimum Length: Passwords must be a minimum of 12 characters in length. For privileged accounts (e.g., administrator, system, service accounts), a minimum length of 15 characters is required. Longer passphrases are strongly encouraged.
* Character Variety (Flexibility over Forced Complexity): While specific combinations of uppercase letters, lowercase letters, numbers, and special characters are not strictly enforced to be present, users are encouraged to create diverse passphrases. Systems will accept all printable ASCII characters, including spaces, and Unicode characters where supported.
  + Recommendation: Create memorable passphrases using a combination of words, or incorporate a mix of character types if creating shorter, more traditional passwords.
* Prohibited Passwords: Passwords must not contain:
  + Commonly used or easily guessable words (e.g., "password," "123456," "qwerty").
  + Company name, usernames, or derivatives thereof.
  + Personal information that is easily obtainable (e.g., birth dates, family names, pet names).
  + Repetitive or sequential characters (e.g., "aaaaaa," "123123").
* Screening: All new passwords will be screened against a database of known compromised passwords and commonly used weak passwords. If a chosen password is found on this list, the user will be required to select a different one.

3.2. Password Management

* Uniqueness: Users must use unique passwords for all [Your Company Name] accounts and systems. Passwords used for company accounts must not be reused for personal accounts, and vice-versa.
* Confidentiality: Passwords must be kept confidential and must not be shared with anyone, including colleagues, supervisors, or IT staff.
  + Do not write passwords down in easily accessible locations (e.g., sticky notes on monitors).
  + Do not share passwords via email, instant messaging, or other unsecured electronic communication.
* Password Managers: The use of a company-approved password manager is strongly encouraged to create, store, and manage strong, unique passwords. Copying and pasting passwords from a secure password manager is permitted.
* Password Change:
  + No Mandatory Periodic Expiration: Users are generally not required to change their passwords at fixed intervals (e.g., every 90 days).
  + Compromise-Driven Changes: Passwords must be changed immediately if there is any suspicion or evidence that the password has been compromised, or if notified by IT security.
  + First-Time Use: Default or temporary passwords must be changed upon first login.
* Password History: Systems will enforce a password history, preventing the reuse of the last 10 passwords.
* Secure Storage: All passwords stored by company systems will be protected using strong, industry-standard cryptographic hashing and salting techniques.

3.3. Account Security

* Multi-Factor Authentication (MFA): MFA is required for all accounts where available, especially for remote access, access to sensitive data, and administrative accounts. Users must enroll in MFA as directed.
* Account Lockout: Accounts will be temporarily locked out after 10 unsuccessful login attempts. Users will need to contact the IT Help Desk to unlock their account.
* Password Hints & Knowledge-Based Authentication (KBA): The use of password hints or KBA (e.g., "What is your mother's maiden name?") for account recovery or authentication is prohibited. Secure, alternative account recovery methods will be provided.
* Session Management: Users must lock their workstations (e.g., by pressing Ctrl+Alt+Del and selecting "Lock" or Cmd+Ctrl+Q on macOS) when leaving them unattended. Users should log off from applications and systems when they are no longer needed.

4. User Responsibilities

* Adhere to all provisions of this password policy.
* Create strong, unique passwords/passphrases as outlined.
* Protect their passwords from unauthorized disclosure.
* Report any suspected password compromise or security incidents immediately to the IT Help Desk or Security Team.
* Utilize company-approved password managers where appropriate.
* Comply with MFA requirements.

5. Administrator Responsibilities

* Ensure systems are configured to enforce this password policy.
* Implement and maintain technologies for password screening and secure storage.
* Provide users with guidance and tools (like password managers) to comply with this policy.
* Regularly review and update this policy to reflect current best practices and threat landscapes.

6. Policy Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract,1 and may also lead to revocation of system access privileges. Violations will be handled in accordance with [Your Company Name]'s disciplinary procedures.

7. Exceptions

Any exceptions to this policy must be documented and approved by [Specify Approving Authority, e.g., Chief Information Security Officer (CISO) or IT Director]. Exceptions will be reviewed periodically.

8. Policy Review

This policy will be reviewed at least annually, or as needed, to ensure its continued relevance and effectiveness.

9. Definitions

* Password: A secret string of characters used to authenticate a user to a system or service.
* Passphrase: A longer sequence of words or other characters used as a password, typically easier to remember than complex short passwords.
* Multi-Factor Authentication (MFA): An authentication method that requires the user to provide two or more verification factors2 to gain access to a resource.3
* Hashing: A one-way cryptographic function that converts a password into a fixed-size string of characters, which cannot be easily reversed.
* Salting: Adding random data to a password before hashing to increase the security of the stored hash.

10. Contact

For any questions regarding this policy, please contact the IT Help Desk or the Information Security Team at [Provide Contact Information].