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

Here's a comprehensive password policy that aligns with modern security best practices and regulatory guidelines (such as NIST SP 800-63B, ISO 27001, and CIS Controls):

**Password Policy**

**1. Purpose**  
This policy establishes minimum requirements for the creation, protection, and management of passwords used to access organizational systems and data.

**2. Scope**  
This policy applies to all employees, contractors, vendors, and third-party users who access the organization's systems, applications, or data.

**3. Password Requirements**

* **Length**: Passwords must be at least 12 characters long.
* **Complexity**: Passwords should include a mix of uppercase letters, lowercase letters, numbers, and symbols. However, complexity rules should not substitute for length or passphrase use.
* **Passphrases**: Users are encouraged to create long, memorable passphrases (e.g., "CorrectHorseBatteryStaple").
* **Blacklist**: Common passwords (e.g., "Password123", "qwerty") and breached passwords must be disallowed using a dynamic password blacklist.
* **No Composition Restrictions**: Do not require arbitrary complexity (e.g., “1 capital, 1 number”) unless required by specific systems, as this reduces usability and does not improve security.

**4. Password Expiry**

* Passwords must not expire arbitrarily (e.g., every 90 days) unless there is evidence of compromise.
* Users must change their password if there is suspicion or confirmation of compromise.

**5. Authentication Methods**

* **Multi-Factor Authentication (MFA)** is required for all remote access and privileged accounts.
* **Biometric and token-based authentication** may be used in addition to passwords for enhanced security.

**6. Storage and Transmission**

* Passwords must be stored using strong, salted hashing algorithms (e.g., bcrypt, Argon2).
* Passwords must never be stored in plaintext.
* Passwords must only be transmitted over encrypted channels (e.g., TLS).

**7. User Responsibilities**

* Users must not share passwords.
* Passwords must not be written down or stored in unsecured files.
* Users must report suspected password compromise immediately.

**8. System Enforcement**

* Account lockout after 10 failed login attempts within 15 minutes.
* Prevent reuse of the last 5 passwords.
* Provide secure password reset mechanisms, such as verified email or MFA-based recovery.

**9. Exceptions**  
Any exceptions to this policy must be approved by the Information Security Team and documented with a valid business justification.

**10. Review and Revisions**  
This policy shall be reviewed annually and updated as necessary to reflect changes in technology, threat landscape, or regulatory requirements.