PASSWORD POLICY TEMPLATE

[Company Name]

Created by Jamola Cybersec Services Limited

1. POLICY PURPOSE

The purpose of this policy is to establish requirements for the creation, management, and protection of passwords used to access [Company Name]'s information systems and data.

2. POLICY SCOPE

This policy applies to all employees, contractors, consultants, and third-party partners who access [Company Name]'s systems, networks, and data.

3. PASSWORD REQUIREMENTS

3.1 Password Complexity Requirements

All passwords must meet the following minimum requirements:

- **Minimum length: 12 characters**
- **Must contain at least one uppercase letter (A-Z)**
- **Must contain at least one lowercase letter (a-z)**
- **Must contain at least one number (0-9)**
- **Must contain at least one special character (!@#$%^&*()_+)**

3.2 Password Expiration

- **Passwords must expire every 90 days**
- **Password history: 10 previous passwords cannot be reused**
- **Users will receive reminders 14, 7, and 1 day before expiration**

3.3 Password Storage

- **-Passwords must never be stored in clear text**
- **Passwords must not be written down or shared**
- **Use a password manager approved by IT**

- Do not store passwords in browser auto-fill

4. ACCOUNT MANAGEMENT

4.1 Account Creation

- All accounts require approval from manager and IT
- Accounts created with least privilege principle
- Default passwords must be changed immediately

4.2 Account Lockout

- Account locks after 5 failed login attempts
- Lockout duration: 15 minutes
- Lockout can be reset by IT support only

4.3 Account Termination

- Access revoked immediately upon termination
- Manager must notify IT within 24 hours
- Account removal from all systems

5. MULTI-FACTOR AUTHENTICATION

- MFA is required for all system access
- MFA methods: Authenticator app, hardware token, or biometric
- SMS-based MFA is not permitted for security reasons

6. RESPONSIBILITIES

6.1 User Responsibilities

- Create and maintain strong, unique passwords
- Report suspected compromise immediately
- Never share passwords with others
- -Use approved password manager
- -Complete annual security awareness training

6.2 IT Responsibilities

- Enforce password policy through technical controls
- Monitor for compromised passwords
- Provide secure password management tools

- **Investigate and respond to password incidents**

7. EXCEPTIONS

Any exceptions to this policy must be:

- **-Requested in writing to the IT Security Manager**
- **Approved by management**
- **Reviewed quarterly**
- **Documented with justification**

8. NON-COMPLIANCE

Failure to comply with this policy may result in:

- **Disciplinary action**
- **Termination of employment - Legal action if applicable**

9. REVIEW AND UPDATES

This policy will be reviewed:

- **-Annually**
- **After any significant security incident**
- **When new threats or vulnerabilities emerge**
- **When regulations or compliance requirements change**

10. APPENDIX A: EXAMPLE COMPLEX PASSWORDS

Strong Password Examples:

- **M@rketing2024$trategy**
- **Secur!tyR0cks#2026**
- **CloudS@fety12!M365**
- **C0mpl3xP@ssw0rd#1**

Weak Password Examples (Avoid):

- **Password123**
- **Admin**
- **CompanyName1**
- **Qwerty123**

APPROVAL SIGNATURES

Policy Owner: _____

Date: _____

Approved by: _____

Effective Date: _____

ABOUT JAMOLA CYBERSEC SERVICES LIMITED

Jamola Cybersec Services Limited provides remote cybersecurity services to SMEs worldwide. We help businesses secure their systems, protect their data, and build resilient security programmes.

Contact: info@jamolacybersec.uk

Website: https://jamolacybersec.uk