Password Policy Template

Password complexity requirements, rotation rules, MFA enforcement, and privileged account management. Define a comprehensive password policy that balances security with usability.

MFA	12+	Passphrase	Free
MANDATORY ENFORCEMENT	MINIMUM CHARACTER LENGTH	MODERN BEST PRACTICE	POLICY TEMPLATE

How to Use This Template

Customise this policy for your organisation, have it reviewed by IT and management, and formally approve it. Communicate the policy to all staff and enforce it technically where possible. Review annually.

1 Policy Overview

Organisation: .....

Policy Version: .....

Approved By: .....

Effective Date: .....

Review Date: .....

Policy Owner: .....

Purpose

This policy establishes the requirements for creating, managing, and protecting passwords across all systems and services used by [Organisation]. It applies to all employees, contractors, and third parties with access to organisational systems.

2 Password Requirements

Standard User Accounts

REQUIREMENT	STANDARD	NOTES
Minimum length	12 characters	Longer passwords are stronger than complex short passwords
Complexity	3 of 4: uppercase, lowercase, numbers, special characters	Or use a passphrase of 4+ random words (16+ characters)
Password expiration	No mandatory rotation (with MFA)	90 days if MFA is not enforced
Password history	Last 10 passwords	Prevents cycling back to previous passwords
Account lockout	10 failed attempts, 30-minute lockout	Prevents brute-force attacks
MFA required	Yes — all cloud services, VPN, and email	Authenticator app preferred over SMS

Privileged / Admin Accounts

REQUIREMENT	STANDARD	NOTES
Minimum length	16 characters	Higher security for higher-risk accounts
MFA required	Yes — mandatory, no exceptions	Hardware token or authenticator app only
Separate from daily account	Yes — admin@domain, not user account	Admin accounts must not be used for email or browsing
Password rotation	Every 90 days	Or use PIM (Privileged Identity Management) for just-in-time access
Session timeout	15 minutes of inactivity	Shorter timeout for higher privilege
Monitoring	All admin actions logged and reviewed	Alert on unusual admin activity

3 Password Management

Rules for storing, sharing, and managing passwords securely.

- **Password manager mandatory:** All staff must use the approved organisational password manager (e.g., 1Password, Keeper, Bitwarden) for storing work passwords.
- **No password sharing:** Passwords must never be shared between individuals. Use shared vaults in the password manager for shared accounts.
- **No written passwords:** Passwords must not be written down, stored in spreadsheets, documents, or sticky notes.
- **No browser storage:** Do not use browser 'remember password' features for work accounts. Use the password manager browser extension instead.
- **Unique passwords:** Every account must have a unique password. Password reuse across services is prohibited.
- **Breach monitoring:** The password manager should be configured to alert on passwords found in known data breaches (Have I Been Pwned integration).

Passphrase Recommended

Modern guidance from NCSC (UK National Cyber Security Centre) recommends passphrases of 3–4 random words over complex short passwords. 'correct-horse-battery-staple' is far more secure and memorable than 'P@55w0rd!'. Enable passphrase guidance in your password policy training.

4 Multi-Factor Authentication (MFA)

MFA requirements for all systems and services.

SYSTEM/SERVICE	MFA REQUIRED	APPROVED METHODS	NOTES
Microsoft 365 / email	Yes	Authenticator app, FIDO2 key	SMS as last resort only
VPN / remote access	Yes	Authenticator app, FIDO2 key	Block if MFA not registered
Admin / privileged access	Yes (enforced)	Hardware token, authenticator app	No SMS, no email codes
Cloud applications (SaaS)	Yes (via SSO)	Inherited from identity provider	SSO reduces MFA prompts
Local workstation login	Recommended	Windows Hello, PIN + biometric	For sensitive roles

5 Enforcement & Compliance

- [ ] Password policy is **enforced technically** via Active Directory / Azure AD / Group Policy
- [ ] MFA is **enforced via Conditional Access** — not reliant on user self-enrolment
- [ ] **Compliance monitoring** identifies accounts not meeting policy (weak passwords, no MFA)
- [ ] **Non-compliance** is escalated to the user's line manager for resolution
- [ ] Policy violations involving **sharing passwords or circumventing MFA** are treated as disciplinary matters
- [ ] Annual **password security training** is provided to all staff as part of security awareness programme

Notes

Need Password Policy Implemented?
Our security team implements password policies, MFA, and password management solutions that protect your organisation.

info@cloudswitched.com
New London House, 6 London St, London EC3R

Prepared by: _____ Date: _____ Approved by: _____

© 2026 CloudSwitched Limited. All rights reserved. This resource is provided for informational purposes and does not constitute professional IT advice.