CLOUDSWITCHED

FREE RESOURCE — PASSWORD POLICY TEMPLATE

Password Policy Template

A ready-to-adopt password policy covering complexity, rotation, MFA enforcement and privileged-account management. Built on NCSC guidance and Cyber Essentials — balancing strong security with usability, and giving you the documented policy auditors, insurers and certification bodies expect to see.

12+	MFA	NCSC	Fillable
MINIMUM CHARACTERS	MANDATORY ENFORCEMENT	PASSPHRASE ALIGNED	TICK & TYPE IN ANY VIEWER

NCSC ALIGNED · CYBER ESSENTIALS · MFA ENFORCED · AUDIT-READY

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

01

Policy overview

This policy establishes the requirements for creating, managing and protecting passwords across all systems and services your organisation uses. Customise the fields below for your organisation, have the policy reviewed by IT and management, then formally approve it. Communicate it to all staff and enforce it technically wherever possible. Review at least annually.

HOW TO USE THIS TEMPLATE

Complete the policy details, confirm the scope, and adapt the requirements in sections 02–04 to your environment. Once approved by management, distribute it to all staff and enforce it through Active Directory / Entra ID conditional access and group policy. Keep the signed copy with your Cyber Essentials evidence pack.

Policy details

Organisation		**Policy version**	
Approved by		**Policy owner**	
Effective date		**Review date**	

Scope — this policy applies to (tick all that apply)

- ☐ All permanent employees
- ☐ Contractors & temporary staff
- ☐ Third parties & suppliers with system access
- ☐ All cloud services & SaaS applications
- ☐ VPN & remote access
- ☐ On-premise servers & workstations

PURPOSE

This policy sets the minimum standard for password security across the organisation. It applies to every account — user, administrative and service — on every system listed in scope above. Non-compliance weakens the organisation's defences against credential theft, phishing and brute-force attack, and is treated as a security matter.

02

Password requirements

Two baselines apply: a standard set for everyday user accounts, and a stronger set for privileged and administrative accounts. These are minimum standards — tighten them if you wish, but never weaken them. Enforce them technically through your identity platform.

Standard user accounts

REQUIREMENT	STANDARD	NOTES
Minimum length	12 characters	Longer passwords are stronger than complex short ones.
Complexity	3 of 4: upper, lower, number, symbol	Or 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 attempts, 30-min lockout	Prevents brute-force attacks.
MFA required	Yes — cloud, VPN & 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 — dedicated admin identity	Admin accounts must not be used for email or browsing.
Password rotation	Every 90 days	Or use PIM for just-in-time access.
Session timeout	15 minutes of inactivity	Shorter timeout for higher privilege.
Monitoring	All admin actions logged	Alert on unusual admin activity.

LENGTH BEATS COMPLEXITY

A 16-character passphrase of random words is far harder to crack — and easier to remember — than an 8-character string of substituted symbols. Favour length over forced complexity.

03

Password management

Rules for storing, sharing and managing passwords securely. These practices remove the most common ways credentials are lost or stolen — reuse, written-down passwords, and insecure sharing.

- **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 or 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. Reuse across services is prohibited.
- **Breach monitoring:** the password manager should alert on passwords found in known data breaches (Have I Been Pwned integration).

PASSPHRASES RECOMMENDED

Modern guidance from the NCSC (UK National Cyber Security Centre) recommends passphrases of three to four random words over complex short passwords. **correct-horse-battery-staple** is far more secure and memorable than **P@55w0rd!**. Include passphrase guidance in your password security training.

MAKE THE SECURE PATH THE EASY PATH

When the approved password manager auto-fills credentials and generates unique passwords on demand, staff stop reusing passwords and stop writing them down — not because the policy says so, but because the tool is easier than the insecure habit. Roll the manager out with the policy, not after it.

04

Multi-factor authentication (MFA)

MFA is the single most effective control against credential theft. The table below sets the MFA requirement and approved methods for each system class. SMS codes are a last resort only — authenticator apps and FIDO2 hardware keys resist phishing far better.

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.

MFA MUST BE ENFORCED, NOT OPTIONAL

MFA that relies on users self-enrolling protects no one — attackers target exactly the accounts that never turned it on. Enforce MFA through conditional access so that registration is mandatory and access is blocked until it is complete. Privileged accounts get no exceptions.

PHISHING-RESISTANT METHODS

FIDO2 security keys and passkeys cannot be phished or replayed the way SMS and one-time codes can. For administrators and high-risk roles, move to hardware keys or passkeys as the primary factor.

05

Enforcement & compliance

Confirm each control below is in place. A password policy is only as good as its technical enforcement — tick each item once it is verified, and raise any gap as an action with a named owner.

- ☐ Password policy is **enforced technically** via Active Directory / Entra ID / 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 the security awareness programme.

REVIEW & OWNERSHIP

Assign one named owner for this policy and put a recurring annual review in the calendar. Re-confirm every control above at each review, and re-run compliance monitoring whenever a new system, supplier or staff cohort comes onboard.

Notes & outstanding actions

06

Sign-off & review schedule

A password policy is only enforceable once management has formally approved it and a next-review date is in the calendar. Complete the fields below, capture the approval signatures, and store the signed copy with your security documentation.

Approval

Organisation name _____

Prepared by (name & role) _____

Date prepared _____

Document version _____

Review schedule

Next full review (12 months) _____

Trigger events for early review _____

Calendar reminder set (Y / N) _____

PREPARED BY	DATE	APPROVED BY (DIRECTOR / IT)

CLOUDSWITCHED

IDENTITY & ACCESS SECURITY

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom