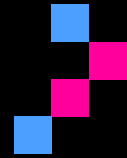


# Password Policy & MFA Implementation Guide



*Initial*  
TECH

## Overview

This plain-English guide helps small and mid-market clients set modern password policies and implement MFA that is resistant to phishing. It adapts the Essential Eight template style and combines recommendations from NCSC, NIST SP 800-63B, CISA ESF, CSA, and Microsoft Entra.

## How to use this guide

- 1) Copy the policy statements into your IT handbook.
- 2) Work through the MFA rollout checklist, ticking Status and pasting screenshots under Evidence.
- 3) Start with admins and high-risk apps; then expand to all users.
- 4) Review quarterly and after major changes.

## 1. Password Policy (modern, user-friendly)

Policy statement	Why (source)	Status / Evidence
<b>Use passphrases of 3+ random words or 14+ characters; allow spaces and normal words.</b>	NCSC: modern password policy reduces burden; NIST 800-63B Rev.4 prefers usability with length over complexity.	
<b>No forced periodic password changes unless compromise is suspected.</b>	NIST 800-63B discourages arbitrary resets; focus on compromise signals.	
<b>Block known compromised passwords and common patterns via screening.</b>	NIST 800-63B requires checking against breach lists; industry practice.	
<b>Enable a password manager and encourage unique passwords per service.</b>	NCSC advocates password managers for businesses and consumers.	
<b>Prohibit shared accounts; use named identities and role-based access.</b>	CISA ESF IAM best practices.	

## 2. MFA Implementation (phishing-resistant first)

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
<b>Prioritise admin &amp; high-value accounts</b>	Start with Global/Privileged admins, finance/HR, and external access. Use Conditional Access templates.		
<b>Require phishing-resistant MFA for admins</b>	Use passkeys/FIDO2, Windows Hello, Platform SSO. Configure Authentication Strength: Phishing-Resistant.		
<b>Block legacy/basic authentication</b>	Disable POP/IMAP/SMTP basic auth; enforce modern auth so MFA applies.		
<b>Create break-glass accounts (excluded from CA)</b>	Two monitored accounts with long random passphrases, hardware MFA if supported; store offline; audit monthly.		
<b>Roll out to all users with friendly onboarding</b>	Use Temporary Access Pass for bootstrapping; provide password manager; explain prompts.		
<b>Enable risk-based controls</b>	Use sign-in risk/device compliance; step-up to stronger MFA when risk rises.		
<b>Set authenticator options hierarchy</b>	Prefer passkeys/FIDO2; allow app-based OTP; avoid SMS/email except as backup.		

### 3. Conditional Access quick template (Entra ID/M365/Azure AD)

- Target roles: Global Admin + other privileged roles.
- Grant: Require phishing-resistant MFA (Authentication Strength).
- Conditions: Block legacy auth; require compliant device for sensitive apps; block high-risk sign-ins.
- Exclusions: Break-glass accounts; service principals.
- Rollout: Report-only → pilot group → phased enforce.

### 4. User education (simple messages)

- Use a password manager; never reuse passwords.
- Expect MFA prompts only when risk changes or on new devices.
- Approve prompts you initiated; report suspicious MFA spam (MFA bombing).
- Prefer passkeys or app-based codes over SMS.
- If locked out, contact IT; do not disable MFA.

### Action plan (next steps)

Action	Owner	Due date	Resources	Status

### References

- NCSC password policy & password manager guidance
- NIST SP 800-63B Rev.4 (authentication & password guidance)
- CISA/NSA ESF IAM best practices (governance, MFA, auditing)
- Microsoft Entra Conditional Access – require phishing-resistant MFA; Secure Future Initiative
- CSA – MFA best practices for seamless journeys