Password Policy Template for UK Small Businesses

Password Policy Template

A password policy helps small businesses protect employee accounts, business data and essential IT systems from unauthorised access. This free password policy template provides a starting point for setting password requirements using password managers enabling multi-factor authentication (MFA) and managing compromised accounts.

Use the template to document your organisations rules assign responsibilities and explain what employees must do to keep business accounts secure.

What you'll find in this template:

- Password creation and secure storage requirements
- Password manager and MFA guidance
- Rules for shared and administrator accounts
- Procedures for compromised or forgotten passwords
- Employee responsibilities and account access reviews
- A checklist, for implementing the policy

What Is a Password Policy?

A Password Policy is a list of rules that tells employees how to create, protect, use and reset passwords for business accounts. A useful Password Policy should cover password length, password reuse, password managers, multi-factor authentication (MFA) account recovery and steps to take if an account is suspected to be compromised.

Why Does Your Business Need a Password Policy?

A written Password Policy helps employees understand how to protect their accounts and gives the business an approach to account security.

It can help your organisation:

- Reduce the risk of account access.
- Discourage password sharing and reuse.
- Encourage password storage.
- Promote MFA on accounts.
- Set a process for reporting suspected account compromise.
- Clarify employee and management responsibilities.

A written Password Policy should be backed by technical controls. Documentation alone cannot secure an account.

Essential Password Policy Rules for Small Businesses

A password policy should explain how employees create, store and protect passwords when accessing company systems. The following rules can be adapted to suit your business.

1. Use Strong Unique Passwords

Employees must use a password or passphrase for each business account. Passwords must not be reused across services or shared with other people.

Where supported systems should block used and known-compromised passwords. Passwords should be sufficiently long. Systems should support practical passphrases and password managers rather than relying on arbitrary combinations of symbols and character types.

2. Use an Approved Password Manager

The business should provide or approve a password manager where appropriate. Employees should use it to generate and store passwords rather than keeping passwords in plain-text documents, spreadsheets or unsecured notes.

Access to the password manager should be protected with MFA where available and access permissions should be reviewed when employees change roles or leave the organisation.

3. Enable Multi-Factor Authentication

MFA should be enabled for business accounts, especially administrator accounts, remote access, email and cloud services.

Where available phishing-resistant authentication methods for high-risk and privileged accounts. Passwords alone should not be treated as protection for critical accounts.

4. Change Passwords When Necessary

Employees must change a password promptly if it is suspected to be compromised, exposed in a data breach or disclosed to a person.

The organisation should not require password changes without a specific security reason. Forced periodic changes can encourage password patterns and unnecessary password reuse.

5. Protect Administrator Accounts

Administrator accounts must be restricted to authorised personnel. Separate administrator accounts from user accounts where appropriate and use MFA and additional monitoring for privileged access.

Default passwords supplied with devices, software or systems must be changed before those systems are put into service.

6. Never Share Passwords Insecurely

Employees must not disclose passwords through email, messaging applications, telephone calls or other unapproved channels.

Where multiple employees need access to the resource use individual accounts and delegated permissions wherever possible. If shared credentials are genuinely necessary, store. Control them through an approved password management solution with suitable access restrictions and auditing.

7. Report Suspected Password Compromise

Employees must report suspected account compromise or unauthorised access immediately using the organisations incident reporting procedure.

The responsible IT team should assess the incident, secure accounts revoke compromised sessions where appropriate reset credentials and investigate possible unauthorised access.

8. Remove Access When Employees Leave

When an employee leaves or no longer requires access the business must. Remove their account and revoke relevant sessions, tokens and permissions as appropriate.

Review shared credentials, service accounts and other access arrangements that may have been exposed to the departing employee. Change affected shared credentials where necessary.

9. Apply Appropriate Technical Controls

The business should use technical controls to reduce password-related risks. These may include MFA, rate limiting, monitoring of login activity, protection against commonly used or compromised passwords and secure password storage by service providers.

Technical controls should be proportionate to the sensitivity of the data and the risk associated with each system.

10. Review the Policy Regularly

The policy owner should review this document periodically and whenever there is a security incident major change to business systems or change, in applicable requirements.

Employees should be informed of updates and the business should retain a record of policy approval and review.

Password Security Checklist for Small Businesses

Use this checklist to check whether your business has the password security controls in place.

Account Security

- □ Employees use passwords for each business account.
- □ Common passwords and passwords that are known to be compromised are blocked whenever the system allows it.
- □ Multi-factor authentication is enabled for business accounts.
- □ Administrator accounts have security controls.
- □ Default passwords have been changed on every system and device.

Password Management

- □ An approved password manager is available when it makes sense.
- □ Employees know how to generate and store passwords securely.
- □ Passwords are not stored in spreadsheets or plain-text documents.
- □ Employees know how to report a suspected password compromise.
- ☐ Password resets use an identity verification process.

Employee Access

- □ Employees understand the password policy and their responsibilities.
- □ Individual accounts are used wherever possible of shared credentials.
- □ Access permissions are reviewed when employees change roles.
- □ Accounts are disabled promptly when employees leave.
- □ Shared credentials are. Updated when necessary.

Monitoring and Review

- ☐ Suspicious login activity is monitored when suitable tools are available.
- □ The business has a documented procedure for compromised accounts.
- □ The password policy has a named owner.
- □ The policy has an approval date and a scheduled review date.
- □ Identified security gaps have assigned owners. Target completion dates.

Asked Questions

- ✷ **Should employees change passwords every month?**

Do not require employees to change passwords every month unless current security guidance or the systems in use justify this requirement. Instead, change a password if it has been compromised or another genuine security reason arises. Always follow the relevant system's requirements.

- ✷ **Should employees use the password for different accounts?**

No. Each account should have its own unique password. Reusing passwords can put multiple accounts at risk if one password is compromised.

A password manager can help users store unique passwords without having to remember every one.

- ✷ **Does a password policy replace MFA?**

No. Multi-factor authentication (MFA) provides an additional layer of protection beyond a password. Enable MFA for accounts wherever the service allows it, especially for email, administrator accounts and other important business services.

Related IT Policy Resources

Explore our Free IT Policy Templates for UK Businesses for policy resources. You might also want to write a Multi-Factor Authentication Policy and an Access Control Policy. These will cover security rules.

Important: This template is a starting point. It is not security advice, for every case. Adapt it to fit your organisation and get advice if you need it.