Passwords

# Passwords

## Overview

This article provides guidance on passwords within the Ministry of Justice (MoJ). It helps you protect MoJ IT systems by telling you about choosing and using passwords. Whenever you see the word 'system' here, it applies to:

* Hardware, such as laptops, PCs, servers, mobile devices, and any IT equipment.
* Software, such as the Operating System, or applications installed on hardware, or mobile device applications (apps).
* Services, such as remote databases or cloud-based tools like [Slack](https://slack.com/).

This password guidance is for all users. It also includes more detail for system administrators or developers.

## Best practices for everyone

The MoJ password guidance follows [NCSC guidance](https://www.ncsc.gov.uk/guidance/using-passwords-protect-your-data). The NCSC recommends a [simpler](https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach) approach to passwords. Some agencies or bodies might have specific requirements or variations. Check your team Intranet or ask your Line Manager for more information.

Follow the [CyberAware advice](https://www.cyberaware.gov.uk/passwords) to generate your passwords. Always use a separate and unique password for each account or service.

The most important points to remember are that passwords should be:

* At least 8 characters long.
* No more than 128 characters long.
* Not obvious.
* Not a dictionary word. A combination of dictionary words might be suitable, such as 'CorrectHorseBatteryStaple'.
* Unique for each account or service.

If a system or another person provides you with a password, change it before doing any MoJ work on that system. Examples of 'single-use' passwords include:

* Your own account on a work-provided laptop.
* A shared account for accessing a data analytics service.
* All supplier or vendor supplied accounts.

You must change a password whenever:

* There has been a security incident involving your account or password. For example, someone guessed your password, or you used it on another account.
* There was a security incident with the service that you access using the password. For example, if someone broke into the system that provides the service you use.
* Your line manager or other authorised person tells you to do so.

When required to change a password, you must do so as soon as possible. If you don't change the password soon enough, you might be locked out of your account automatically. The following table shows the maximum time allowed:

|  |  |
| --- | --- |
| Type of system | Maximum time to change a password |
| Single-user systems, such as laptops | 1 week |
| All other systems | 1 day |

## Password expiry

You don't have to change a password because it is old. The reason is that time-expiry of passwords is an [...outdated and ineffective practice](https://www.ncsc.gov.uk/blog-post/your-password-expiry-policy-may-have-reached-its-expiry-date).

Some current or legacy systems don't allow passwords that follow MoJ guidance. For example, some mobile devices, laptop hard drive encryption tools, or older computers might not be able to support a mix of character types. For such systems, choose passwords that are as close as possible to MoJ guidance.

## Password managers

Use a password manager to help you keep track of your passwords.

These are tools that help you create, use, and manage your passwords. A useful overview is available [here](https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers).

As passwords become more complex, and you need to look after more of them, it becomes increasingly necessary to use a password manager. For example, development teams in MoJ Digital & Technology use [LastPass](using-lastpass.html).

You still need to remember one password. This is the password that gets you into the manager application. Once you have access, the application works like a simple database, storing all the passwords associated with your various accounts and services. Some managers have extra features, such as password generators. Some managers can even automatically fill-in username and password fields for you when during log in.

The password manager database is often stored in the cloud so that you can use it anywhere. The database is encrypted, so only you can open it. That's why your single password key is so important. Without it, you can never get access to the password database again.

Using a password manager for your MoJ account and service details is recommended.

You can find additional useful information about password manager tools [here](password-managers.html).

Extra guidance for system administrators or developers is available [here](https://www.ncsc.gov.uk/guidance/helping-end-users-manage-their-passwords).

## System administrators or developers

Follow the [Government Service Manual for Passwords](https://www.gov.uk/service-manual/design/passwords) when you administer or develop MOJ systems or services.

Suppliers and vendors must ensure that systems support the password requirements. Systems must be able to issue, change, reset, and revoke passwords. This must be possible using well-defined and fully-described processes. Supply enough information and procedures to fulfil MoJ password policy.

The [NCSC guidance](https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach) for simplifying passwords says that forcing complex passwords has:

* Marginal security benefit.
* A high user burden.

Technical controls are more effective at protecting password-based authentication. Examples include:

* [Locking accounts](#password-access-attempts) after repeated access attempts.
* [Blocking](#blocking-bad-passwords) common password choices.

### Related guides

Further guidance around the management of passwords at the MoJ is available:

* The [Account management](account-management.html) guide explains why you might need to change your password. It also addresses when and how you should change your password.
* The [Multi-User Accounts and Public-Facing Service Accounts Guide](multi-user-accounts-and-public-facing-service-accounts-guide.html) explains when you should use a multi-user account and how you should authenticate a service account.
* The [Password Creation and Authentication Guide](password-creation-and-authentication-guide.html) helps ensure you choose the correct passwords and authentication tools to protect information in line with its security classifications.
* The [Password Storage and Management Guide](password-storage-and-management-guide.html) provides help on storing and sharing passwords securely.

## User facing services

Authenticate people accessing user facing services by using the [GOV.UK Verify](https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify) service. It is not necessary for someone to be a UK Citizen to use the GOV.UK Verify service, but they must have a UK address.

If it is not possible to use GOV.UK Verify, follow the advice presented here to support citizen passwords. Pay extra attention to the following points:

* People should have complex passwords which are different for each service they use. Make it easy for people to have complex passwords by supporting password managers. For example, services should always let users paste passwords into web forms.
* Don't force [regular password expiry](#password-expiry). Make it easy to [change passwords](#password-reset) when required.
* Do force password changes when required. For example, after [exceeding a count of unsuccessful password entry attempts](#password-access-attempts).
* Make the process of [resetting a password](#password-reset) like providing a password for the first time. Include a way to [prevent attackers using the reset process](#distributing-passwords-to-users) to conduct an attack.

For more information, see the [Multi-user accounts and Public-Facing Service Accounts Guide](multi-user-accounts-and-public-facing-service-accounts-guide.html).

## Service Accounts

System and application authentication must always use service accounts. Use certificates for service account authentication. Follow [NCSC guidelines](https://www.ncsc.gov.uk/guidance/provisioning-and-securing-security-certificates) for issuing and securing the certificates. If you can't use certificates, passwords are an acceptable alternative.

Service account passwords must:

* Be system generated.
* Be at least 15 characters long.
* Be no more than 128 characters long.
* Be complex, including upper-case and lower-case letters, digits, punctuation, and special characters.
* Be kept secure, by using hashes or encryption.
* Not be stored in the clear in any systems or applications.
* Not be used by standard or administrative users for any purpose.

For more information, see the [Multi-user accounts and Public-Facing Service Accounts Guide](multi-user-accounts-and-public-facing-service-accounts-guide.html).

## Default passwords

Change all default passwords when a new, modified, or replacement system arrives. Complete the changes before making the system available for any MoJ work.

## Multi-factor Authentication

[Multi-factor Authentication (MFA)](https://en.wikipedia.org/wiki/Multi-factor_authentication) provides extra security for login and access controls. MFA is also referred to as Two-Factor Authentication or 2FA.

Use MFA in systems for privileged or important step confirmation. For example, the user must enter their MFA code when deleting a record.

Follow the [NCSC guidance](https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services) for enabling MFA.

Use [Time-based One-Time Password Algorithm (TOTP)](https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm) or hardware and software tokens. If possible, avoid using SMS or email messages containing one-time login codes. If TOTP applications, or hardware- or software-based tokens, are not available to you, then SMS MFA or email MFA is still better than no MFA.

Systems must offer MFA alternatives to users where they are available. For example, MFA codes sent by SMS are not suitable if mobile devices are not allowed in the room or building.

For more information, see the [Multi-Factor Authentication (MFA) Guide](multi-factor-authentication-mfa-guide.html).

## Extra measures

Check that a system, service, or information protected by a password is not [classified](official-official-sensitive.html) as SECRET or TOP SECRET. Make sure that it doesn't contain delicate material. Examples include contracts, or personal data or information. If it does contain such material, you might need extra access control.

Check which other systems have access to the system or service. Make sure that the access control suits the material at both ends of the connection.

Appropriate extra measures might include tokens or other multi-factor authentication devices. Think about using an existing authentication system other than passwords. Avoid creating new authentication systems. Try to reduce what a user must remember. For more information about authentication, see the [Authentication](authentication.html) guide.

A technical risk assessment helps identifies extra controls for systems. This is mandatory for systems that need formal assurance. Multi-user systems are also subject to a Business Impact Assessment (BIA). For example, an assessment might find that you need extra checks for logging in to an account or service. The checks might depend on various factors such as:

* Time of login.
* Location of login.
* Number of previous connections from the connecting IP address.
* Whether to allow more than one login at a time.

Examples of these extra mechanisms include:

* Biometrics.
* Tokens.
* Certificate-based authentication.

## Password storage

Never store, display or print passwords [in the clear](https://en.wikipedia.org/wiki/Plaintext). If you must store them, do so by using [salted](https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet#Use_a_cryptographically_strong_credential-specific_salt) [hashes](https://en.wikipedia.org/wiki/Hash_function).

Ensure the password storage security matches the [classification](official-official-sensitive.html) of the system or data. For help with the appropriate strength of hashing, contact the Cyber consulting team: [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk), or the security team: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk)

Extra information on handling and protecting passwords is in the [Password Storage and Management](password-storage-and-management-guide.html) guide.

## Password access attempts

If a password is ever entered incorrectly, a count starts. After at most 10 (ten) consecutive failed attempts at using the correct password, access to the account or system is locked. A successful use of the password resets the count to zero again.

## Password reset

If a password lock occurs, a reset is necessary. This requires action by the system administrator or the MoJ Service Desk. The process should be like issuing the password for the first time. Other account details are not changed during the reset. This helps avoid losing any work. Checks ensure that an attacker cannot use the password reset process.

## Blocking bad passwords

You should not try and use [obvious passwords](https://en.wikipedia.org/wiki/List_of_the_most_common_passwords). Attempts to do so will be blocked.

Developers and administrators should configure systems to check for and block obvious passwords embedded within a password. For example, MySecretPassword is not a good password! Use password and hash lists from [SecLists](https://github.com/danielmiessler/SecLists/tree/master/Passwords) or [Have I Been Pwned](https://haveibeenpwned.com/Passwords), to help prevent bad passwords.

## Distributing passwords to users

There are times when a system must send a password to a user. An example is when granting access to a service for the first time. To send a password to a user, the mechanism used must be secure. The protection should match the sensitivity of the information protected by password.

Passwords created for a user should always be [single-use](#single-use-passwords). Use an out-of-band channel to send the password to the user. For example, send the password to the user's line manager who will give it to the user.

For more information, see the [Password Storage and Management Guide](password-storage-and-management-guide.html).

## Single-use passwords

Some passwords are 'one time' or single-use. Administrators and developers use these to grant access to a service for the first time. After using the password once, the user must immediately change the password.

Single-use passwords are time limited. If they are not used within a specific time after generation, they must become invalid.

The following table shows the valid lifetime of a single-use password:

|  |  |
| --- | --- |
| Type of system | Lifetime of a single-use password |
| Single-user systems, such as laptops | 1 week |
| All other systems | 1 day |

## Multi-user systems and services

All multi-user systems and services must check for redundant User IDs and accounts. If necessary, remove the redundant IDs or accounts.

The [Access Control Guide](access-control-guide.html) discusses the management and removal of accounts.

If someone is no longer allowed to access a system, check for and change any shared account or common password they might still have.

For more information, see the [Multi-user accounts and Public-Facing Service Accounts Guide](multi-user-accounts-and-public-facing-service-accounts-guide.html).

## Identity Providers and Single Sign-On

When you need an authentication solution, try to use existing MoJ services. Examples include Identity Provider (IdP) or Single Sign-On (SSO) services, such as Office 365 or Digital and Technology G-Suite.

This helps reduce the need to design, create, deploy and manage yet another solution.

SSO integration in existing IdP solutions improves the user experience. This is because you can authenticate to systems using existing MoJ credentials.

For more information, see the [Multi-user accounts and Public-Facing Service Accounts Guide](multi-user-accounts-and-public-facing-service-accounts-guide.html).

## Account management

This guidance on passwords is separate from the guidance on account management. You should still follow the rules and processes for managing accounts. In particular, while you don't need to [change passwords after a period of time](#password-expiry), you should still expire accounts promptly. Examples would be when accounts are no longer required, or have fallen out of use.

For more information, see the [Account management](account-management.html) guide.

## Contact details

For any further questions relating to security, contact: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk), or for security advice, contact the Cyber Assistance Team [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).