#Passwords

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.

##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 |

##App-based password protection for files

Some applications provide a mechanism for protecting files, for example by using a password to control whether someone can open, or edit, a file.

While these app-based password protection mechanisms are better than nothing, there are three good reasons for avoiding them if possible.

1. You depend on the application to provide and maintain strong password protection. If the password implementation fails, or has a weakness, you might not know about it. This means that you might think your information is protected, when in fact it is at risk.
2. It is tempting to use a standard password for protecting a file within the app, so that other people can share and work with the file. Changing the password becomes “inconvenient”. The result is that many versions of the data file are all protected with the same password. Also, if anyone has ever been given the password to access the file, they will always be able to access the file.
3. If you forget the app-based password, there might not be a recovery process available to you.

For these reasons, MoJ advice is that you **SHOULD NOT** use password tools within an app to protect data files that are processed by the app. Instead, either:

1. Store the data files in a shared but secure area, such as the MoJ SharePoint storage facility.
2. Use separate encryption tools to protect data files, separate from the app that works with the data files.

Of these two options, storing data files in a shared but secure area is strongly preferred. The reason is that you can add, modify, or revoke access permissions to the storage area easily.

If you have no choice, and have to use app-based password protection, ensure that the same password is not used indefinitely for a data file. You **SHOULD** use a different password for:

* Each major version of a data file, for example version 2.x is different to version 3.x.
* Any data file where the password is more than three months old.

**Note:** This advice is a specific exception to the [general guidance](#password-expiry), that you do not normally need to change passwords.

##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](/guidance/security/it-computer-security/user-access/passwords/password-managers/using-lastpass-enterprise/).

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](/guidance/security/it-computer-security/user-access/passwords/password-managers/).

##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.

##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.

##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 |

##Contacts

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

##Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).