Password Storage and Management Guide

# Password Storage and Management Guide

## Introduction

Do not attempt to implement your own password storage mechanism. Always use an existing, approved Ministry of Justice (MoJ) password storage solution.

This guide sets out how passwords must be stored securely to prevent unauthorised access or compromise. The MoJ encourages the use of password managers to reduce the burden on users for maintaining password security. For more information, see the [Password Management Guide](password-management-guide.html).

This guide has been written in alignment with [NCSC guidance](https://www.ncsc.gov.uk/collection/passwords/updating-your-approach).

## Password storage

Passwords must be securely stored within MoJ approved storage tools. The following tool is approved and preferred for use:

* [LastPass](using-lastpass.html)

Contact the Cyber Assistance Team ([CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk)) if you have a specialist need to use a different storage tool.

## Sharing passwords

Passwords should not normally be shared. Sharing of passwords should be avoided by delegating privileges to other accounts, for example to provide access to a document or inbox.

Passwords can be shared for the following exceptions:

* For an encrypted document that has to be shared to make sense.
* For generic administration accounts on third-party services or applications, which support only a single account for administration purposes. If multiple individuals will perform the role, then the account password would have to be shared. [Privileged Access Management (PAM)](privileged-account-management-guide.html) should be used where possible for systems that are administration only.

Some applications, for example, some social media tools, do not have 'role awareness'. This means you can't have access associated with a role; it must be through an individual account. This is sometimes 'solved' by having a PAM tool, where the PAM tool provides a more comprehensive managed 'gateway' to the underlying tool.

If there is a strong business need for shared access to a resource, account or system, then access to the password should be monitored and continually reviewed. This would be performed by:

* Regular auditing of who should have the password.
* Access revocation by changing the password if someone should no longer have access.
* Using proactive monitoring where it is enabled, for example by cross-referencing instances where the password is used with the dates and times that an authorised person could be using the password.

A shared password must be:

* Governed by PAM, and only be used by known and trusted users.
* Changed if any user in the group is no longer allowed access.
* Shared using a password manager.

## Password vaults and managers

A password vault is a tool that stores passwords and other high-value secrets or credentials in an encrypted form. A password manager provides extra user-friendly tools for working with a password vault, for example helping you log in to applications or websites using the credentials stored within the vault. Password managers allow you to keep track of multiple passwords and avoid weak passwords.

The MoJ prefers [LastPass](using-lastpass.html) for Team use, or business use by an individual.

Some teams, particularly service development and administration, have specialised needs that make other password vault tools more suitable. These project-specific tools include:

* AWS Key Management
* Azure Key Vault
* Hashicorp Vault
* Kubernetes Secrets

For further guidance on password strength, see the [Password Creation and Authentication Guide](password-creation-and-authentication-guide.html). Contact the Cyber Assistance Team [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk) if you have a specialised need to use a different password manager or vault.

## 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).