Password Management Guide

# Password Management Guide

## Introduction

This guide sets out the roles and requirements for setting and maintaining strong passwords across Ministry of Justice (MoJ) systems.

The information is aimed at two audiences:

* The in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects and Service Owners. It also includes Incident Managers from the [Event, Problem, Incident, CSI and Knowledge (EPIC) team](https://peoplefinder.service.gov.uk/teams/epic).
* Any other MoJ business group, agency, contractor, IT supplier and partner who in any way designs, develops or supplies services (including processing, transmitting and storing data) for, or on behalf of the MoJ.

## Roles and responsibilities

### All MoJ Digital and Technology users

Everyone must ensure that password creation, distribution and maintenance is done securely.

Passwords must not ordinarily be shared. Refer to the [Password Storage and Management Guide](password-storage-and-management-guide.html) for exceptions and alternative solutions for sharing passwords.

Passwords must be strong and complex. Refer to the [Password Creation and Authentication Guide](password-creation-and-authentication-guide.html) for more details.

Passwords must be changed upon indication of compromise.

Passwords must be distributed securely. Refer to the [Password Storage and Management Guide](password-storage-and-management-guide.html).

Multi-factor authentication (MFA) must be enabled for existing systems, wherever possible. MFA must be enabled for new systems. Further guidance can be found in the [Password Creation and Authentication Guide](password-creation-and-authentication-guide.html) and the [Multi-User Accounts and Public-Facing Service Accounts Guide](multi-user-accounts-and-public-facing-service-accounts-guide.html).

Where a default password is applicable, it must never be guessable.

### Software Developers, Technical Architects and Development Operations

Make every effort to avoid creating yet another new or modified password-based authentication system. If it is unavoidable, then ensure that the following security requirements are adhered to:

* Multi-user accounts should be avoided, but if required refer to the [Multi-User Accounts and Public-Facing Service Accounts Guide](multi-user-accounts-and-public-facing-service-accounts-guide.html) for further guidance.
* Technical controls must be implemented to support requirements in the [Password Creation and Authentication Guide](password-creation-and-authentication-guide.html).
* Applications or software must support MFA, and where possible single sign-on (SSO) solutions leveraged by the MoJ.
* Passwords must not be stored in clear text or using encryption algorithms with known security weaknesses.
* Passwords must not be transmitted in clear text over networks.
* All applications or software must use HTTPS to require authentication.
* Applications or software must provide some form of role management, whereby an authorised user can take over the functions of another without having to know the other users' password.
* Passwords and other secrets (SSH Keys, DevOps secrets, etc.) must never be embedded into applications. The use of key vaults, such AWS Secrets Manager, is strongly recommended.
* Where a default password is applicable, it must never be guessable.

### Suppliers and vendors

Suppliers and vendors must ensure that their systems support the password requirements set by the MoJ.

Supplier or vendor systems must be able to change, reset and revoke passwords. This must be possible using well-defined processes.

Suppliers and vendors must implement the technical controls in the MoJ guidance, such as locking accounts after repeated access attempts and blocking common password choices, to improve the effectiveness of password-enforcement and compliance.

Senior Business Owners for Contracts should ensure that when contracts are signed, the supplier receives explicit guidance on password management and it is included in the associated contractual Security Management Plan (SMP).

### System Administrators

System Administrators (SAs) must ensure that systems support the password requirements set by the MoJ. When provisioning and maintaining user accounts, SAs must:

* Require a change of initial or first-time passwords.
* Verify a user's identity before resetting a password.
* Implement automated notification of a password change or reset.

SAs must also ensure privileged accounts:

* Are authorised only for a specified time.
* Are managed and regularly reviewed for user access, so that access is revoked when a user no longer needs it. This is to prevent unauthorised access.
* Use MFA for user authentication.
* Have activity logs for the purposes of review and monitoring.

## 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.

## 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).