Account management

# Account management

## Introduction

This guide provides help on account management, for example when passwords should be changed or when user accounts should be locked. For more information, see the [Password Management Guide](password-management-guide.html).

The information is aimed at two audiences:

* The in-house 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 Ministry of Justice (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.

## Account lockouts

Account lockouts must be implemented within MoJ systems for the following reasons:

Failure to change passwords within the allocated time.

Systems must have a ‘change password’ function to recover the account or contact information for the Technology Service Desk.

Unsuccessful connection attempts.

Allow no more than 10 consecutive login attempts before lockout.

Forgotten passwords.

All MoJ systems must have a forgotten password link on the login page, enabling the user to change the password on their own. Ensure this uses multi-factor authentication for user verification.

Removed or revoked access.

Users may experience account lockouts due to inactivity, need to know permissions or change of employment status such as contract termination. Access to these accounts must only be re-enabled with line manager approval.

Systems should have a way to forcibly revoke an account, and disconnect any active session instantly. This is to deal with scenarios such as suspicion that an account or access has been compromised. The session disconnect is required because revoking an account on some systems does not necessarily invalidate an existing session immediately.

## Password changes

When designing and developing systems for use within the MoJ, password changes must be enforced for these events:

* A user has forgotten their password or is experiencing login issues.
* There has been a security incident involving the account or password.
* An authorised person, such as line manager or IT support, requests the change.
* The system prompts you to change a password.
* You suspect an account might have been compromised.

Password changes must be made within the following timeframes:

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

## Revoking accounts

All MoJ user accounts are access controlled according to the user's 'need to know' requirements and their employment status. Accounts should be revoked at contract termination and during long-term absences, such as maternity or long-term sickness leave. The MoJ revokes user accounts in alignment with the [Access Control Guide](access-control-guide.html).

## 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).

## Feedback

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