Access Control guide

# Access Control guide

## Introduction

This guide explains how the Ministry of Justice (MoJ) manages access to its IT systems so that users have access only to the material they need to see. This guide has sub-pages which provide in-depth Access Control guidance.

## Who is this for?

This guide is aimed at two audiences:

1. The in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation.
2. 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.

## Related guides

Further guidance on how to manage user access can be found in the guides below.

* [Privileged Accounts](privileged-account-management-guide.html).
* [Management Access](managing-user-access-guide.html).
* [Minimum User Clearance Requirements](minimum-user-clearance-requirements-guide.html).
* [Multi-Factor Authentication (MFA)](multi-factor-authentication-mfa-guide.html).

## Information security principles for access control

These are the Access Control principles you need to know.

* **The 'need-to-know' principle:** Restricting access to information based on a business requirement.
* **Non-repudiation of user actions:** Holding a user accountable for their actions on an IT system.
* **The 'least privilege' principle:** Assigning the least number of privileges required for users to fulfil their work, usually done through Discretionary Access Controls (DAC).
* **User Access Management:** Managing user access to systems and services through a formal user identity lifecycle process.

## Access control principles

Effective access control should be implemented by following these four principles.

1. **Identification:** The MoJ should provide a single, unique ID assigned, named and linked to a private account for each user. For example, Lesley is issued a user account that only Lesley uses, and only Lesley can access. This is important so that logging information is accurate (see the [Accounting section below](#access-control-principles__accounting) for further information).
2. **Authentication:** To access MoJ systems, users must authenticate themselves. They can do so using:
   * something they know (such as a password - the primary authentication method used at the MoJ)
   * something they have (such as a smart card)
   * something they are (biometric authentication such as a fingerprint, voice recognition, iris scan and others)

* Systems holding sensitive information, or systems that are mission critical to the MoJ, must use Multi-Factor Authentication (MFA) to prove user identity. See the [Multi-Factor Authentication Guide](multi-factor-authentication-mfa-guide.html) and [Password Management Guide](password-managers.html) for further information. If you wish to use an additional method of authentication you should review the National Cyber Security Center's (NCSC) guidance and contact the Cyber Assistance Team (CAT). For information on authentication methods including OAuth, refer to the [Managing User Access Guide](managing-user-access-guide.html).

1. **Authorisation:** Authorisation is the function of specifying access rights/privileges and resources to users, which should be granted in line with the principle of least privilege. Reducing access privileges reduces the "attack surface" of IT systems. This helps to prevent malware and hackers from moving laterally across the network if they compromise a user account.
2. **Accounting:** Successful and unsuccessful attempts to access systems, and user activities conducted while using systems must be recorded in logs. Please see the [Security Log Collection Guide](security-log-collection-maturity-tiers.html) for more information. This will help to attribute security events or suspicious activities to users who can be supported to improve their behaviours or held accountable for their actions.

Consider the following points when creating activity logs.

Logs should be:

* stored securely
* backed up, so that data are not lost if there is a system unavailability
* managed according to the sensitivity of the data they hold, for example personal information. Contact the Data Privacy Team for advice on protecting sensitive personal information - [privacy@justice.gov.uk](mailto:privacy@justice.gov.uk).
* stored for a minimum of 6 months

Logs should not be:

* retained for longer than 2 years unless otherwise stipulated. Retention rules may vary on a case by case basis so check with the Data Privacy Team, the Cyber Assistance team, and the MoJ Data Protection Officer if a Log involves personal information. See the [Accounting Guide](accounting.html) for further information.
* tampered with under any circumstances, for example through modification or removal.

See the [Security Log Collection Guide](security-log-collection-maturity-tiers.html) for more information.

## Segregation of duties

In some parts of the MoJ, segregation of duties is used to help to reduce the possibility that malicious activity takes place without detection.

You can segregate duties in various ways, including:

* implementing manual or automated Role Based Access Control (RBAC), to enforce user authorisation rights.
* regularly reviewing audit logs to check for suspicious activity
* ensuring strict control of software and data changes
* requiring that a user can perform only *one* of the following roles:
  + identification of a requirement or change management request (Business function)
  + authorisation and approval of a change request (Governance function)
  + design and development (Architect or Developer function)
  + review, inspection, and approval (another Architect or Developer function)
  + implementation in production (System Administrator function)

## Contact details

Contact the Cyber Assistance Team for access control advice – [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk)