Privileged Account Management Guide

# Privileged Account Management Guide

## Introduction

This guide explains how to manage privileged accounts in order to minimise the security risks associated with their use. This is a sub-page to the [Access Control Guide](access-control-guide.html).

## How to manage privileged accounts

Holders of privileged accounts, such as system administrators, have privileges to perform most or all of the functions within an IT operating system. Staff should have privileged accounts only when there is a business need, in order to prevent malicious actors gaining privileged access to Ministry of Justice (MoJ) systems. The MoJ requires that ownership and use of privileged accounts must be monitored and audited on a monthly basis.

Privileged accounts should be protected with the following controls.

|  |
| --- |
| DO |
| ✔ Ensure that privileged users only use their system administrator account when elevated privileges are required. Their general user account should be used for all other work activities. |
| ✔ Ensure that management or administrative access is limited to users who have been suitably authenticated and have been authorised to perform the specific action. Only those with a genuine business need should have an administrative account, however there should be a sufficient number of administrators that there is not a single point of failure due to absence or administrators leaving the MoJ. This should be enforced through the principle of least privilege. |
| ✔ Ensure that Multi Factor Authentication (MFA) is used where possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. MFA should also be used to access enterprise level social media accounts. See the [Multi-Factor Authentication Guide](multi-factor-authentication-mfa-guide.html) for details of preferred MFA types. Where MFA cannot be used on a system, this is considered an exception and should be logged in the risk register. |
| ✔ Ensure that MFA is mandated for a privileged user to conduct important or privileged actions such as changing fundamental configurations including changing registered email addresses or adding another administrator. |
| ✔ Ensure that MFA is used as a validation step, to confirm actions requested by users, such as a MFA re-prompt when attempting to delete or modify data. |
| ✔ Ensure that default passwords are managed securely and safely, as described in the [Password Manager guidance](password-managers.html). |

|  |
| --- |
| DON'T |
| ✖ Allow privileged users to use their privileged accounts for high-risk functions. These include reading emails, web browsing, using an 'administrator' login on an end-user device (such as a mobile device), or logging into a server as 'root'. |
| ✖ Leave default or factory set passwords for any accounts but particularly for privileged system accounts, social media accounts and infrastructure. |
| ✖ Allow a user to have a privileged account, unless they are a service provider and require a privileged account for that specific service. |

## Contact details

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