Multi-user accounts and Public-Facing Service Accounts Guide

# Multi-user accounts and Public-Facing Service Accounts Guide

## Introduction

This guide sets out when multi-user accounts should be used, although this is discouraged and should be avoided if possible. The guide also explains how public-facing service accounts should be authenticated. 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).

## Multi-user accounts

In this context, a multi-user account is where a single set of credentials is used by more than one person. This can be found on legacy systems where there is a dedicated administrator account. Multi-user accounts allow multiple users with individual logins and varying permissions to use the same account. Multi-user accounts need to be managed carefully using [Privileged Account Management](privileged-account-management-guide.html) (PAM) or a Bastion server to avoid security risks associated with accountability. Multi-user accounts should only be used directly if there is no alternative.

Note: A [Bastion server](https://en.wikipedia.org/wiki/Bastion_host) is a specially strengthened system that provides access to parts of the Ministry of Justice (MoJ) private network from an external network, such as the Internet. It provide specific access to to a well-defined set of servers or services, rather than permitting general access across the network.

The multi-user account checklist requires that you:

* Undertake a Business Impact Assessment (BIA) before implementation of a multi-user account to understand risks posed to the MoJ.
* Note: The BIA provides details on how the business views the impact to their information assets and services following a loss of Confidentiality, Integrity or Availability. This is useful because it provides a steer on what types of incidents result in the highest impact to the business and how tolerant the business is to a loss of service provision. For help on creating a BIA, contact the Cyber Assistance Team: [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).
* Create a pre-defined and authorised list of users.
* Implement using the 'need to know' access principle on the PAM. Alternatively, if using a bastion host, see what options there are to enforce this principle.
* Regularly check for redundant user IDs and accounts on either the PAM or bastion hosts. These should then be blocked or removed.

## Public-facing services

Developers and administrators should ensure that front-end users who access the MoJ public-facing services or applications are authenticated through the GOV.UK Verify Service. When this is not possible, for example when an individual does not have a UK address, passwords must:

* Be easy to use, for example, pasting passwords into web forms should be enabled.
* Not be forcibly changed simply as a result of a period of time passing. However, passwords and other account access mechanisms must be revoked for an individual when they are no longer authorised to work with the account.
* Use Two Factor Authentication (the [Password Creation and Authentication Guide](password-creation-and-authentication-guide.html) provides further advice).
* Be changed when required, for example after a system compromise is identified, or if the limit of unsuccessful password attempts is reached and the account is locked.
* Be reset using a one-time password.

The [Password Creation and Authentication Guide](password-creation-and-authentication-guide.html) provides further guidance creating a strong and complex password.

## Service accounts

Service accounts must be used for system and application authentication at a privileged level. Service accounts must use certificates for authentication, however if these cannot be used, then passwords are an acceptable alternative. The [Password Creation and Authentication Guide](password-creation-and-authentication-guide.html) provides further guidance on how you must create a strong and complex password.

## 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).