1. Introduction

This User Management Policy is a sub-policy of the Information Security Policy (ISP-01) and sets out the requirements for the effective management of user accounts and access rights. This management is essential to ensure that access to the University’s data and information systems is restricted to authorised users.

2. Scope

This policy applies to all information systems used to conduct University business, or which are connected to the University network.

This applies to all members of the University (staff, students and associates) and members of other institutions who have been granted permission to use the University’s information systems.
3. Policy

3.1. Eligibility

User accounts will only be provided for:

- Current university staff and students.
- Emeritus staff and those who have otherwise been granted honorary status.
- Associate staff, including members from other organisations that provide services to
  the University who may require access to the University’s information systems to fulfil
  their contractual obligations.
- Students waiting to graduate.
- Guests of the University who may be granted temporary access to the University’s
  network.
- Visitors to the University who may be granted temporary access to the University’s
  wireless network.

The University may also provide access to a limited range of services to its alumni,
prospective students and job applicants.

3.2. Authorisation to manage

The management of user accounts and privileges on the University’s information
systems is restricted to suitably trained and authorised members of staff.

3.3. Account and privilege management

Accounts will only be issued to individual users that are eligible for an account and
whose identity has been verified.

When an account is created, a unique identifier (userID) will be assigned to the individual
user for their individual use. This userID may not be assigned to any other person at any
time (userIDs will not be recycled).

On issue of account credentials, users must be informed of the requirement to comply
with the University’s Information Security policies.

Access rights granted to users will be restricted to the minimum required in order for
them to fulfil their roles.

Procedures shall be established for all information systems to ensure that users’ access
rights are adjusted appropriately and in a timely manner to reflect any changes in a
user’s circumstances (for example when a member of staff changes their role or a
member of staff or student leaves the University).

Privileged or administrative accounts are accounts used for the administration of
information systems and are distinct from user accounts. These accounts must only be
used by system administrators when undertaking specific tasks that require special
privileges.

System administrators must use their standard user account at all other times.
Periodic audits of privileged accounts must be conducted in addition to the regular maintenance of accounts (and not only when members join, move or leave).

3.4. Password management

As part of the account provisioning process, the user may need to be informed of an initial, temporary password. This password must be communicated to the user in a secure way and must be changed by the user immediately. This change should be enforced automatically wherever possible.

3.5. Multi-Factor Authentication

Users may be asked to present additional evidence as well as their password to authenticate themselves to University systems. This is referred to as Multi-Factor Authentication (MFA).

Additional evidence requested would likely be in the form of either a one-time code sent to a phone or non-University email address, or a question and answer response based on previously supplied information.

Information given to the University for MFA will be stored securely and only used for authentication purposes. It will be stored by the University or a University trusted provider and will not be provided to any third party without the user’s written consent, unless the University is required to do so by law.

All administrative or highly privileged accounts must have Multi-Factor Authentication enabled where available.

4. Further Guidance

Guidelines for system and network administrators: https://www.bristol.ac.uk/media-library/sites/infosec/documents/sysadmin.pdf