University of Bristol
Information Security Policy

Title:	**User Management**
Reference:	**ISP-08**
Status:	**Approved**
Version:	**1.1**
Date:	**September 2017**
Review:	**February 2019**
Classification:	**Public**

Contents

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 in order to ensure that access to the University's information and information systems is restricted to authorised users.

Scope

All information systems used to conduct University business, or which are connected to the University network, must be managed in accordance with this policy.

Eligibility

User accounts will only be provided for:

- Current university staff and students.
- Emeritus staff and those who have otherwise been granted honorary or associate status (associates will include staff from other organisations which provide services to the University who may require access to the University's information systems in order to fulfil their contractual obligations to the University.)
- 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.

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.

Account and privilege management

Accounts will only be issued to those who 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 (userID's will not be recycled).

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

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 (e.g. when a member of staff changes their role or a member of staff or student leaves the University).

Privileged 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 which require special privileges. System administrators must use their user account at all other times.

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.

Multi-Factor Authentication

Users may be asked to present additional evidence other than their password to authenticate themselves to University systems. This is referred to as Multi-Factor Authentication (MFA). The use of MFA greatly improves the security of user's accounts along with the data and systems they access. The reliance on MFA is borne from the increased likelihood of a user's password being compromised and the use of internet services that do not require a user to be on campus to access.

Additional evidence requested would likely be in the form of either a one-time code sent to a phone or non-UoB 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 your prior written consent, unless we are required to do so by law.