Identity and IT Access Management Policy

Purpose and Context

This policy defines the required access control measures to all University information technology (IT) systems and applications to protect the privacy, security, and confidentiality of University IT resources, systems, and data.

Scope

This policy applies to identities and access controls put in place across University of Huddersfield (UoH) IT systems and resources. It covers identities, permissions, systems, and resources that are managed both centrally and elsewhere in the University across students, staff, affiliates, and any other category of person who may have access to IT systems and resources.

1.0 Introduction

This policy defines the required access control measures to all University information technology (IT) systems and applications to protect the privacy, security, and confidentiality of University IT resources, systems, and data. It defines the range of electronic identities that are centrally managed and the responsibility for any identities belonging to non-centrally managed IT systems.

The Identity and Access Management (IDAM) policy mandates that controls exist to:

- Ensure that a new user is who they say they are, and the level of trust and access given to them is commensurate with their personal and professional background.
- Bind an identified user to an identifier within systems with an appropriate method of authentication.
- Ensure that the authentication method gives confidence that when an identifier is used, it is being used by the member of staff whose identity has been previously validated.
- Apply the principle of least privilege to limit the access or functionality that different users have.

2.0 Concepts

2.1 Identification

Identification is the process of assigning digital identifiers to each individual to enable decisions about the level of access to IT systems that should be granted. Identifiers should:

- **Be unique to the individual.**
  They should uniquely identify a single person. They should not be shared between individuals. A direct link between the identifier used to access a system and a particular person should exist.
  An exception may exist for top-level “global” administrative accounts, though these should be an access mechanism of last resort.
- **Be singular to the individual or role.**
  Each individual should normally have one and only one identifier in any given system. However, there may be occasions where an individual has more than one identifier in a system, for example if they have multiple distinct roles within the University or the system. Examples might include a staff member who is also a student, or a staff member who uses

a system as a privileged administrator, but also uses the system as a non-privileged "end user".

- **Not be reassigned.**
  An identifier should never be re-used for a person other than the originally identified individual.
  A rare exception may exist for top-level "global" administrative accounts, though these should be an access mechanism of last resort.

The validation of individual's identities is performed by:

- The Human Resources team for staff members.
- Admissions teams (including International) for students and applicants.
- The sponsoring individual for affiliates and other accounts.

Computing and Library Services (CLS) are responsible for creating central identifiers for individuals and do so in good faith that the information provided by those validating identities is accurate and their requests appropriate.
System Owners are responsible for the process by which identifiers are created in their own systems, and for ensuring that identities have been validated.

2.2 Authentication

The authentication process determines whether someone or something is the genuine owner of the identifier that they are presenting. Authentication validates the identifier and therefore the individual who owns that identity.

Authentication relies on the owner of an identifier presenting private information known only to the individual owner of that identifier such as a PIN or password. It may also rely on something the individual has – a multi-factor authentication (code generator) app, for example. The identifier itself is not considered private information.

In the text of this policy reference will be made to "passwords", but this policy recognises that other valid modern authentication mechanisms exist. References to "passwords" should be considered to include these and the principles of this policy should be honoured in their intent where the direct statements made do not apply outside of the context of a traditional password.

To maintain the security of the authentication process, all systems **must**:

- Use encrypted communication mechanisms for authentication.
- Not store credentials in clear text within the system.
- Not use default passwords. Any default passwords should be changed as soon as practicable.
- Where the system manages authentication credentials locally within the system, allow users to select their own password and to change any password assigned to them.
- Implement multi-factor authentication if possible and require use of this if accessed through the Internet.
- Implement password minimum length constraints that ensure a reasonable level of password complexity.
- Lockout an identifier after no more than 10 unsuccessful attempts.
- Record successful and unsuccessful authentication attempts.

All systems **should**:

- Use centrally provided identification and authorisation mechanisms such as Active Directory or Azure Active Directory where possible.
- Not use predictable password schemes unless unavoidable. Initial passwords should be generated to be unique and random.
- Require users to change upon first authentication any initial password they have been allocated.
- Use an irreversibly encrypted form for password storage if storage is required.
- Not require individuals to periodically create a new password.
- Allow use of “pass phrases” which could be comprised of recognisable words, and not require password complexity measures such as special symbols and numbers.
- Automatically reject the setting of common passwords.
- Enforce password history controls to prevent the reuse of previous passwords.

Individuals **must**:

- Never reveal or share their password or other secret information to others.
- Immediately change their password or other secret information if they have reason to believe it has become known to another person.
- Set a unique password for any system that does not link to central mechanisms. It is not permitted to reuse passwords across multiple University or non-University systems.

2.3 Authorisation

Authorisation is the process used to grant permissions in or to a system or resource to an authenticated identifier, and ergo an identified individual. Authorisation determines and applies the level of access a particular authenticated identifier should receive in the system or resource (e.g. which records can be read and/or written to). It is the role of the system or application to determine if the identifier has permission to perform the requested operation, though this may be based upon role definitions passed to it by other systems (e.g. Active Directory group membership).

It is a role of the System Owner to determine appropriate levels of authorisation for the data and business processes within their systems and to establish rules for how these authorisation levels will be allocated to individuals or roles.

- A principle of least privilege should be applied. Individuals should only be allowed the levels of access and permission required to do their job or fulfil their authorised purpose.
- Where feasible, a “just in time” grant of elevated privilege should be applied, whereby an identity has additional rights applied only for the duration of a particular activity.
- Privileges should be removed when an individual changes role or otherwise no longer needs these privileges.
- System Owners should maintain records of changes to privilege levels or, if this is automated, documentation should exist on the decision-making process within the automation.
- System Owners must review authorised identities and their permissions within their systems periodically.

2.4 Segregation of Privileges

Some individuals by nature of their roles within the University or their responsibilities in relation to IT systems may find that they act as both an administrator of a system and an end user of the system. Use of a single identifier in these cases may lead to a breach of the principle of least privilege – for example, an administrator logging on to the HR system to book their own annual leave may receive an unnecessarily privileged level of authorisation for their purpose on that occasion.

To avoid this a principle of segregation of privileges will apply in accordance with best practice guidance from the UK Government's National Cyber Security Centre (NCSC). Technical or administrative users who need a high level of authorisation within a system to perform their technical roles will maintain a separate identifier for this purpose, distinct from their identifier as an end-user of a system. Normally a central University identifier will be used to access systems as an end-user, and one or more separate identifiers will be created for administrative and technical work. Individuals maintaining such a separate, privileged identifier must ensure that a distinct and strong password is used for this identifier, different to that used for their primary identifier.

All other principles of identifier allocation, authentication, and authorisation apply to these additional identifiers, including but not limited to the fact that there should be a one-to-one relationship between the identifier and an owning individual.

2.5 Defunct Identities

All identifiers related to identities that are "defunct" in the context of the University must be removed or disabled, including any additional privileged identifiers created for the purposes of segregation of privileges. Identities are considered defunct where:

- The individual corresponding to that identity has left the University.
- The individual no longer has a role that requires access to IT facilities.
- The individual changes role e.g. from Student to Staff, or from Affiliate to Staff.
- The individual has moved role from one School, Service, or major Organisational Unit to another.

In the latter of these cases, it is possible that a new identity will be created for the individual in their new role should it require access to IT facilities. This helps to constrain the proliferation of privileges from one role to another.

Identities that are considered defunct should be identified by:

- The Human Resources team in the case of staff.
- The Student Records team in the case of students and prospective students.
- The sponsoring individual in the case of affiliate and other accounts.

CLS are responsible for removing or disabling defunct identifiers in centrally managed IT systems.

System owners are responsible for removing or disabling defunct identifiers in their own systems.

3.0 Roles and Responsibilities

3.1 RACI Definitions

The RACI matrix defines the responsibilities and accountabilities related to this policy.

R = Responsible; A = Accountable; C = Consulted; I = Information Receiver

Responsibility and Accountability roles are singular, meaning one role is the focal point for execution and measurement.

The roles of consultant and information receiver may be performed and received by multiple participants.

Responsibility

Those with an “R” in the matrix hold responsibility for execution of the process and are engaged to perform one or several tasks. One main role is Responsible to perform a task. When other groups or organizations also have responsibility for the execution of the process, they are considered as having secondary responsibility and as such are given a designation of “r” on the RACI Matrix. An example would be of a process that is executed by both IT and one of our service providers. IT holds the primary responsibility (R); the service provider has secondary responsibility (r).

Accountability

Those with an “A” in the matrix hold accountability for the output of the process and its quality. This role may engage other resources to perform the execution but is ultimately accountable for the result and quality. Only one role is assigned Accountability.

Roles that have accountability for an activity must ensure that the task is done.

3.1 RACI Matrix

Activity	Computing and Library Services	System Owners	HR	Admissions Teams	Affiliate sponsors	Individual “User”
Validate an individual’s identity	I	I	R, A	R, A	R, A	C

Activity	Computing and Library Services	System Owners	HR	Admissions Teams	Affiliate sponsors	Individual “User”
Allocate identifiers	R, A	R, A	I		I	I
Ensure uniqueness of identifiers	R, A	R, A				
Ensure a one-to-one relationship between identifiers and individuals	R, A	R, A	R	R	R	C
Ensure identifiers are not re-allocated	R, A	R, A				
Establish a process for identifier allocation	R, A	R, A				
Ensure authentication mechanisms are encrypted	R, A	R, A				
Ensure that systems do not store authentication	R, A	R, A				

Activity	Computing and Library Services	System Owners	HR	Admissions Teams	Affiliate sponsors	Individual "User"
secrets in clear text						
Ensure that default passwords are changed	R, A	R, A				
Implement MFA	R, A	R, A				C
Ensure passwords meet a minimum length standard	R, A	R, A				C
Minimise privilege levels	R, A	R, A				C
Ensure privileges are removed when an identity changes role	R, A	R, A				
Maintain records of privilege level changes / how decisions are made	R, A	R, A				

Activity	Computing and Library Services	System Owners	HR	Admissions Teams	Affiliate sponsors	Individual “User”
Periodically review authorised identities	R, A	R, A				C
Apply segregation of privileges	R, A	R, A				C
Identify when identities are no longer required	I	I	R, A	R, A	R, A	
Remove access for defunct identifiers	R, A	R, A				I

POLICY SIGN-OFF AND OWNERSHIP DETAILS	
Document name:	Identity and IT Access Management
Version Number:	1.0
Equality Impact Assessment:	19 June 2023
Privacy Impact Assessment:	July 2023
Approved by	Senior Leadership Team
Date Approved:	29 June 2023
Date for Review:	June 2026
Consulted with (Departments / Area of Service / Job Title):	CLS IT Management Team CLS IT Support Manager CLS IT Service Desk Manager CLS Senior Management Team HR System Owner Information Security Champions
Author:	Deputy Director and Head of IT
Owner (if different from above):	Deputy Director and Head of IT
Document Location:	https://www.hud.ac.uk/media/policydocuments/Identity-And-IT-Access-Management.pdf
Compliance Measures:	Biennially request outcomes of user audit from a selected system owner.
Related Policies/Procedures:	IT Security Policy

REVISION HISTORY			
Version	**Date**	**Revision description/Summary of changes**	**Author**
V1.0		First release of new policy	Deputy Director and Head of IT