Identity, Access Control and Account Management Policy

Policy Owner:	**Title:** Director of Digital Technology Services		
Approved by:	**Committee\individual:** Information Governance and Security Oversight Group **Date:** 31 July 2023		
Directorate\team:	**Directorate:** Digital Technology Services **Team:** DTS Security **Contact details:** email ! SHU IT Security		
Last Review	July 2023		
Version	1.1		
Amendments since Approval:	**Details of Revision:**	**Date of Revision:**	**Revision Approved by:**
	Merge of Identity and Access Management Policy with Access Control and Account Management Policy. Some links are internal where they relate to staff and students.		

1. Policy Statement

Sheffield Hallam University is responsible for ensuring the confidentiality, integrity, and availability of its data and that of personal data stored and processed on its systems. The University has an obligation to provide appropriate governance of the use of user accounts across its systems. These controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their specific purpose.

2. Objectives

The objective of this policy is to ensure the University has adequate controls in place to restrict access to systems and data, to describe how controls should be used and to provide a basis for enforcement of these controls.

3. Purpose

The purpose of the policy is to specify the University's policy on access management. This policy has been developed to explain what controls should be in place to limit access to information and ensure that users only have rights to appropriately authorised information systems and applications. Protecting access to IT systems and applications is critical to maintaining the integrity of University technology and data and prevent unauthorized access.

4. Scope

This policy applies to:

- Any user who accesses University IT systems networks and application
- Any service that is accessed onsite, hosted services and data centres either onsite or cloud based.
- All IT systems and applications managed by the University, including network and computer hardware, software, mobile devices, and telecommunications systems.

5. Definitions and Abbreviations

"Access Control" is the process that limits and controls access to resources of a computer system.

"Users" are students, employees, consultants, contractors, agents, visitors, and authorized users accessing University IT systems and applications.

"System or Application Accounts" are user IDs created on IT systems or applications, which are associated with specific access privileges on such systems and applications.

"Privileged Accounts" are system or application accounts that have advanced permissions (as compared to regular user account permissions) on such systems or applications. Examples of user accounts with privileges include administrative and super user accounts.

"Access Privileges" are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, install, or remove applications, etc.

"Administrator or Super User Account" is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, install applications, maintain patching, etc.

"Application and Service Accounts" are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.

"Nominative User Accounts" are user accounts that are named after a person.

"Guest Accounts" or "Visitor" are short term user accounts created for events.
"Visitors" are persons using the University facilities, IT services or applications, that are not members of the University as employees, students or under any other contract with the University.

"Generic or Shared Accounts" are user accounts which are shared among multiple persons or devices.

"MFA" means Multi Factor Authentication

6. User Responsibilities

- All users are bound by the Universities Regulations for the use of IT Facilities and the Janet Acceptable Use Policy.
- Users must not share login details with any other person.
- Users must not use the passwords or login details of another user without approval of Director of DTS.
- Passwords must be unique and comply with the Password policy
- Staff are required to change their password in line with the University Password policy
- Admin Accounts (ADM accounts) must not be used as your primary means of logging onto the network, or to access external sites, resources, or email as if compromised this could give malicious actors administrative rights to SHU resources.
- Remote access to private SHU systems and applications must use the University VPN service and/or MFA.
- When a member of staff changes role, the new line-manager is responsible for Change of Role requests for access and the old line-manager is responsible for the removal of access.
- Visitors under the age 18 will be required to provide a written undertaking of legal responsibility from their parent or guardian before being given access.

7. Policy Details

General Requirements

- The University will provide access privileges to University technology (including networks, systems, applications, computers and mobile devices) based on the following principles:

  - Need to know – users or resources will be granted access to systems that are necessary to fulfil their roles and responsibilities.

  - Least privilege – users or resources will be provided with the minimum privileges necessary to fulfil their roles and responsibilities.

- Requests for user accounts and access privileges must be formally documented and appropriately approved.
- Accounts are to be set up for individuals and not to be shared. When a generic or role-based username is required, a shared account may be created but only for specific purposes which are recorded along with the details of individual users for tracking purposes.

- Student accounts shall be created for the students when they have accepted a place of programme of study and are regarded as provisionally enrolled. Access will include University IT services, such as Filestore, email account and student portal that are required for their studies.

- All staff shall have individual accounts, for privacy and accountability, which will be created at the request of the line manager.

- Requests for special accounts and privileges (such as vendor accounts, application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by the system owner and the requestor's line manager.

- Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administrators or application developers only.

- Where possible, the University will set user accounts to automatically expire at a pre-set date. More specifically,

  - When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.

- User accounts assigned to contractors will be set to expire according to the contract's expiry date.

- VPN accounts assigned to external supplier or support will be enabled for an agreed period, to complete contracted project tasks, contracted development tasks, perform investigation or approved change. The account must be disabled on completion of the task if this is before the end of the defined active period.

- Student accounts will be set to expire/deleted at the end of their course, however limited access to certain systems may be granted until conferment.

- Student accounts shall be deleted if the student is withdrawn from the course.

- Staff accounts will be set to expire where the period of employment is defined.

- Access rights will be immediately disabled or removed when the user leaves the University or ceases to have a legitimate reason to access University systems.

- Access rights may be disabled or restricted:
  - If student fees have not been paid
  - For disciplinary reasons (staff and students)
  - If a user account is known or suspected to have been compromised

- A verification of the user's identity must be performed by IT Help before granting a new password or suspending MFA.

- Students on very short courses and visitors may use temporary accounts. The Service Desk shall be responsible for maintaining a log of these accounts to ensure adherence to the University IT Regulations.

- Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts and accounts with excessive privileges. Identified dormant accounts will be disabled and/or deleted. Active accounts with excessive privileges will have those privileges removed. Examples of dormant accounts include:

  - An active account assigned to external contractors, vendors or employees that no longer work for the University.

- Systems and application sessions must automatically lock after a defined period of inactivity.

Privileged Accounts

- Privileged accounts will only be granted where there is benefit to the University.

  - Privileged rights may be withdrawn by DTS is they are not used in accordance

with this policy.

- Privileged accounts must only be used for the tasks that require elevated rights. They must not be used for general day-to-day activities, which include reading email or web browsing.

- The need for a privileged account will be reviewed with the owner every year and the account removed if the requirements for elevated rights are no longer valid. Users will need to positively state their continued need for a privileged account, failure to respond to requests for justification will result in the elevated rights being withdrawn.

- A nominative and individual privileged user account must be created for administrator accounts, generic administrator account names must not be used.

- Privileged user accounts can only be requested by managers or supervisors and must be appropriately approved and specific to the administrative access required.

- Passwords for privileged accounts must not match passwords for any other account held by the nominated privileged account holder.
- Global Administrator Privileges will only be granted on case-by-case basis with the aim of restricting this to a small number of staff to reduce the security risk.

Local Workstation Administrator Accounts

- Users granted Local Workstation Administrator (LWA) accounts that meet the criteria above (**Privileged Accounts**), must abide by the following, failure to do so may result in the LWA account being removed:

  - Users must not add their normal user account or any other account to the Administrators Group on the workstation.

  - Users must not use the LWA account or any other administrative account for day- to-day activities, which includes reading email or web browsing.

  - LWA accounts must not be used to remove or disable software installed on workstations, including anti-virus tools or management agents. These are critical to ensuring the workstation is kept up-to-date and is as secure as possible.

  - Users must not remove other users from the workstation Administrators Group. However, if additional administrative user accounts are created as the result of the LWA account being used to install software, then they are an exception to this rule.

Generic or Shared User Accounts

- Where possible, the use of groups should be used for common access permissions

across multiple users, and not shared accounts.

- Shared user accounts are only to be used on an exceptional basis with the appropriate approval. This includes general user accounts such as “guest” and “functional” accounts.

- When shared accounts are unavoidable:

  - Passwords will be stored securely and handled in accordance with the Password Policy

  - The use of shared accounts for example: guest accounts, will be logged and records may be accessed when required, including the recording of the time of access, the reason for accessing the shared user account, the length of time the account is required, and the individual accessing the account. When the shared user account has administrative privileges, such a procedure is mandatory and access to the monitoring logs must be protected and restricted.
  - Accountability and retention of the data for shared accounts resides with the owner(s) of the account or the person(s) requesting the accounts.
  - The use of MFA will not be required on shared accounts.

Vendor or Default User Accounts

- Where possible, all default user accounts will be disabled or changed. These accounts include “guest”, “temp”, “admin”, “Administrator”, and any other commonly known or used default accounts, as well as related default passwords used by vendors on “commercial off-the shelf” systems and applications.

- Vendor or default privileged accounts must not be used except in emergencies or when appliances, systems or applications are first deployed, to create nominative accounts, or where it is not possible to create alternative privilege accounts.

Test Accounts

- Test accounts can only be created if they are justified by the application/service owner or project team and approved by the application owner, through a formal request via the Service Desk.

- Test accounts must have an expiry date. Maintaining test accounts beyond this date must be re-evaluated and approved appropriately.

- Test accounts will be disabled and/or deleted when they are no longer necessary or no longer in use.

Contractors and Vendors

- Contracts with contractors / vendors should include specific requirements for

the protection of data. In addition, contractor / vendor representatives will be required to agree to the University IT Security policies, in particular the IT Regulations, before being granted access to University systems and applications.

- The name of the contractor / vendor representative and access requirements must be communicated to the Service Desk at least 2 business days before the person needs access.

- The University will maintain a list of external contractors or vendors having access to University systems.

- The need to terminate the access privileges of the contractor/vendor must be communicated to the Service Desk at least 1 day before the end of access is needed.

Exceptions to this Policy

- Exceptions to this policy must be documented and formally approved by the Security Assurance Manager Policy exemptions must describe:
    - The nature of the exception with a reasonable explanation for why the policy exception is required.
    - Any risks created by the exception and any compensating controls.
    - Duration of the exception or review frequency.
    - Evidence of approval of the exception.

- Alternative authentication mechanisms that do not rely on a unique user account and password must be formally approved as an exception to this policy.

Misuse and Abuse

- All instances of misuse or abuse of the University IT systems, actual or suspected, shall be reported as soon as possible to IT Help and subsequently to the Security Team
- All investigations into breach of this policy shall be conducted using the University Problem Resolution Framework or the Student Disciplinary Procedures and records of the investigation kept, according to the best practices guidelines.

8. Roles Responsibilities

Roles	Responsibilities
DVC (Strategy Operations)/SIRO	• Approve and formally support this policy
Director of Digital Technology Services	• Review and formally support this policy. • Respond to reports of policy breaches or misuse of IT resources.
Security Assurance Manager	• Review and formally support this policy. • Approve and maintain records of exceptions.

DTS Security Team	• Develop and maintain this policy. • Actively enforce compliance for all stakeholders with this policy.
DTS	• To review and support the policy. • Annual review for dormant and excessively privileged accounts. • Annual review of the need for privileged accounts.
University Staff	• Ensure that students are aware of the policy at enrolment. • Support all staff, students, and other users in understanding the requirements of this policy. • Immediately report any instances of non-compliance with this policy to the Service Desk.
Service Desk/IT Help	• Assign requests for the creation, modification, or removal of accounts to the appropriate team for the request, within 1 working day. • Assign notifications of non-compliance of this policy to the DTS Security Team.
Human Resources and Organisational Development	• Present each new employee with the relevant University IT and Security policies before they commence work. • Support all employees and students in understanding the requirements of this policy.
All Users	• Review this and other policies regularly to keep their understanding of their responsibilities up to date. • Report all instances on non-compliance with this policy to a member of staff or the Service Desk as soon as possible.