Sheffield Hallam University

Identity and Access Management Policy

Issuing Authority: Simon Briggs,
Director of Digital Technology Services

Signed: 

Date Effective: February 2022

Review date: February 2023

Version: 2022.6

Identity and Access Management Policy

Document Control

Version number	Authors	Notes	Date
2022.6	Dave Ainscow	First Issue	31/01/2022

Introduction

Sheffield Hallam University is responsible for ensuring the confidentiality, integrity, and availability 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 and services to ensure that security risks are not created by the delegation of privileges. Effective implementation of this policy will limit the exposure and effect of common attacks and threats to the systems within this scope.

Policy

1. Policy Requirements

1.1. Protecting access to IT systems and applications is critical to maintain the integrity of the Sheffield Hallam University ("SHU", or "University") technology and data and prevent unauthorised access to such resources.

1.2. Access to University systems and data, must be restricted to only authorised users or processes, based on the principle of strict need to know and least privilege.

2. Background

2.1. Access controls are necessary to ensure only authorized users can obtain access to the University's information and systems.

2.2. Access 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 job roles.

3. Policy Objective

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

4. Scope

4.1. This policy applies to:

4.1.1. All University offices, classrooms, open access areas, campuses, hosted services and data centres either on site or Cloud based

4.1.2. All staff, students, consultants, contractors, agents, visitors and authorized users accessing University IT systems, networks and applications.

4.1.3. All IT systems or applications managed by the University that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems

5. Definitions

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

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

5.3. "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.

5.4. "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.

5.5. **"**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.

5.6. **"**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.

5.7. **"**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.

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

5.9. "Guest Accounts" are short term user accounts created for events and/or "Visitors". These accounts are restricted in their access.

5.10. "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.

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

6. Guiding Principles – General Requirements

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

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

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

6.2. Requests for user accounts and access privileges must be formally documented and appropriately approved.

6.3. 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.

6.4. 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.

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

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

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

6.5.3. 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.

6.5.4. Student accounts will be set to expire at the end of their course.

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

6.6. 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.

6.7. A verification of the user's identity must be performed by the Helpdesk before granting a new password.

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

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

6.8.2. Active accounts assigned to students that have either completed their course or are no longer considered members of the University. For example, where a student drops out of their course prior to completion.

6.8.3. An active account with access rights for which the user's role and responsibilities do not require access. For example, where users have moved from one team to another where systems from their previous role should not remain accessible.

6.8.4. System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator.

6.8.5. Unknown active accounts.

6.9. All access requests for system and application accounts and permissions will be documented using the Helpdesk system in place.

7. Guiding Principles – Privileged Accounts

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

7.1.1. Privilege rights may be withdrawn by DTS is they are not used in accordance with this policy.

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

7.1.3. Elevated rights will be reviewed every year and removed if the requirements for a privilege account are not met. Users will need to positively state their continued need for a privilege account, failure to respond to requests for justification will result in the elevated rights being withdrawn.

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

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

7.4. Passwords for privilege accounts must not match any other account held by the nominated privilege account holder.

8. Guiding Principles – Local Workstation Administrator Accounts

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

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

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

8.1.3. 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.

8.1.4. 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.

9. Guiding Principles – Generic or Shared User Accounts

9.1. Where possible, the use of specific network domain "security groups" should be used to share common access permissions across many users, instead of shared accounts.

9.2. Shared user accounts are only to be used on an exception basis with the appropriate approval. This includes general user accounts such as "guest" and "functional" accounts.

9.3. When shared accounts are required:

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

9.3.2. The use of shared accounts will be monitored where possible, including the recording of the time of access, the reason for accessing the shared user account, and the individual accessing his 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.

10. Vendor or Default User Accounts

10.1. 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.

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

11. Test Accounts

11.1. Test accounts can only be created if they are justified by the relevant business area or project team and approved by the application owner, through a formal request to the IT Help Desk.

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

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

12. Contractors and Vendors

12.1. 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.

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

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

12.4. The need to terminate the access privileges of the contractor / vendor must be communicated to the IT Help Desk at least 1 business day before the contractor / vendor representative's need for such access ends, or immediately should the contracted work be completed ahead of schedule.

13. Access Control Requirements

13.1. All users must use a unique usercode to access University systems and applications. Passwords must be set in accordance with the Password Policy.

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

13.3. Remote access to University systems and applications must use the University VPN service and/or multifactor authentication where possible.

13.4. System and application sessions must automatically lock after a defined period of inactivity.

14. Multifactor Authentication (MFA)

14.1. All University supported services and applications should enforce MFA where authentication is required and MFA is possible.

15. Exceptions to the Policy

15.1. Exceptions to the guiding principles in this policy must be documented and formally approved by the DTS Security Team. Policy exceptions must describe:

15.1.1. The nature of the exception with a reasonable explanation for why the policy exception is required.

15.1.2. Any risks created by the exception.

15.1.3. Evidence of approval of the exception.

16. Roles and Responsibilities

Roles	Responsibilities
Director of Digital Strategy	• Approve and formally support this policy
IT Security Officer	• Review and formally support this policy
DTS Security Team	• Develop and maintain this policy • Actively enforce compliance for all stakeholders with this policy • Review and approve any exceptions to this policy • Maintain a record of approved exceptions and associated risks
CNI Identity Management Team	• Review and administer accounts, privileges and access group membership.
University Staff	• 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 Desk	• 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	• Present each new employee or contractor with the relevant University IT and Security policies before they commence work with the University. • 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 and in line with any changes • Report all instances on non-compliance with this policy to a member of staff or the Service Desk as soon as possible