Password and Authentication Policy

Policy Owner:	**Title:** Director of Digital Technology Services		
Approved by:	**Committee\individual:** Information Governance and Security Oversight Group **Date:**		
Directorate\team:	**Directorate:** Digital Technology Services **Team:** DTS Security **Contact details:** email ! SHU IT Security		
Last Review	January 2025		
Version	1.3		
Amendments since Approval:	**Details of Revision:**	**Date of Revision:**	**Revision Approved by:**
	Review and reformat to current SHU policy standards in line with other University policy formats and incorporate MFA.		
	Amendment to include Clear text	30/01/2025	

- ## Policy Statement

  Sheffield Hallam University is committed to ensuring that its systems and data are secure and protected from unauthorised use. To support this, all users must take appropriate steps to protect the user account they are provided. This will include choosing a strong and secure password and setting up additional verification methods where services require Multi Factor Authentication (MFA). MFA provides additional protection against the possibility that usernames and passwords are obtained by unauthorised users.

  Intentional sharing of usernames and passwords or otherwise enabling unauthorised use of a user account may be treated as a breach of the University IT Regulations and lead to disciplinary action being taken.

  You should not use your university password for any other external service(s) and should choose a strong and unique password for each service.

  The University may force users to change their password if there is a risk your account is being misused.

- ## Objectives

  The objective of this policy is to set out the requirements for authentication methods needed to access University applications and services.

- ## Scope

  This policy applies to:

  - All Users
  - All University services and applications

- ## Definitions and Abbreviations

  "Multifactor Authentication (MFA)" is the process of using more than one piece of evidence (or factors) to prove who users are when they sign in to applications and/or services.

  "Users" are students, staff, consultants, contractors, agents, visitors, and any other authorised users of University IT systems and applications.

  "Clear text Passwords" are passwords that are stored and/or transmitted in an unencrypted format.

- ## Policy Details

  ### General Requirements

  - User passwords must be a minimum of 12 characters and include a combination of 3 of the 4 different character types (upper case, lower case, numbers and special characters).
  - Users should not use the previous 8 passwords when setting a new password
  - Passwords must not be a single dictionary word.

- Passwords must not contain the users first name, surname, username, employee or student number.
- Passwords should not be based on easily identifiable information, for example a pet's name.
- Six incorrect login attempts will lead the account being locked out for 30 minutes.
- Any user that thinks their account(s) is/are at risk must change their password as soon as they can, for example your account being used by someone else or you are subject to a phishing email.
- All passwords must be treated as confidential and must not be shared with anyone or made public in any form – either written or verbally.

See Appendix 1 for advice on choosing and setting a strong password.

- **Exceptions**

  - To ensure the security and integrity of our systems and data users must not store or send credentials (passwords, keys etc) in clear text on networked devices. This includes but is not limited to use of emails, document files, SharePoint and configuration files.
  - Any user that is required to transmit a password outside the University must ensure that it is encrypted beforehand, either on suitable storage or file formats, or by transmitting only over secure channels (e.g. HTTPS, SSH).
  - Other exceptions to this policy will be considered on a case-by-case basis.

- **Roles and Responsibilities**

Roles	Responsibilities
Security Assurance Manager	• Review and approve any exceptions to this policy
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	• Report any risks or concerns about their password or user account to the Service Desk • Report any instances of non-compliance with this policy to the Service Desk • Support other users in understanding the requirements of this policy
Student Academic Services	• Present students with relevant University IT policies prior to enrolment. • Support all students in understanding the requirements of this policy.