UNIVERSITY OF HULL

Password and MFA Policy

Classification:	Policy
Version Number:	2.0
Status:	Approved
Approved by (Board):	University Leadership Team
Approval Date:	22 February 2022
Effective from:	22 February 2022
Next Review Date:	Annual
Document Authors:	Steph Jones, Nigel Kavanagh
Document Owner:	Security and Architecture Manager, ICT (Steph Jones)
Department/Contact:	support.hull.ac.uk
Summary:	This document outlines the password and Multi-Factor Authentication (MFA) policy and guidance for all University members and third parties to which is applies
Scope:	All University members and third parties required to authenticate with University ICT systems and services
Collaborative provision:	Not applicable
Assessment: (where relevant)	Not applicable
Consultation: (where relevant)	Not applicable
Relevant legal frameworks:	See relevant section of overarching Information Governance and Assurance Policy
Related documents:	Information Security Controls Policy
Published locations:	Public website (www.hull.ac.uk)
Document Communication and Implementation Plan:	Available upon request.

All printed versions of this document are classified as uncontrolled.
A controlled version is available from the university website.

Password and MFA Policy

1. Introduction

1.1. This document outlines the password and Multi-Factor Authentication (MFA) policy and guidance for all University members and third parties to which it applies. This policy has been derived from the controls referenced by the **Information Security Controls Policy** and guidance from the National Cyber Security Centre (NCSC).

1.2. All University ICT systems use password authentication as a minimum. The University uses Single-Sign-On (SSO) where possible so that a user can authenticate seamlessly against multiple services.

1.3. Recognising the limitations of passwords, core ICT systems and services such as email, cloud file storage, and remote access, will be protected by Multi-Factor Authentication (MFA). Information systems owned by departments and faculties shall be protected by MFA where possible.

2. Scope

2.1. This policy applies to all University members and third parties required to authenticate with University ICT systems and services. University members include staff, students, visitors and other associate roles.

2.2. This policy applies to standard users. Additional requirements for privileged users/administrators, and system specific accounts, are defined in controls approved and managed by the ICT department.

3. Passwords

3.1. All University members and third parties shall set a unique password for their University account and not use (re-use) the password for any other services, whether personal or work/study-related.

3.2. All University members and third parties will protect their password and not share them with other users. The use of delegated and/or shared access should be deployed instead, following advice from ICT.

3.3. Passwords shall be at least 12 characters in length, although longer passwords or passphrases are recommended. There is no maximum password length.

3.4. Passwords will not be subject to complexity requirements.

3.5. Passwords must not contain the user account name or any other personally identifiable information (date of birth, address, name of pet, for example).

3.6. Passwords must not be based on commonly used passwords. Where possible, technical controls should enforce this restriction. Passphrases, including groups of random words are recommended as an alternative. Further guidance and examples can be found from the NCSC. [1]

[1] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

3.7. All University members and third parties must notify ICT if they know or suspect that their password has been compromised. They must change their password as soon as they can.

3.8. Newly set passwords should not be the same as, or similar to, previously used passwords. Where possible, technical controls should enforce this restriction.

3.9. Passwords will not expire arbitrarily. This is in accordance with best practice guidance from the NCSC.[2]

3.10. Passwords will be changed without notice when in response to a security incident or where ICT monitoring detects suspicious activity.

3.11. University members are recommended to generate and store credentials in a password management solution of their choice. Popular password managers include KeePass, Bitwarden, LastPass and 1Password, however, users should be aware of the risks of doing so. Further guidance can be found from the NCSC.[3]

4. Multi-Factor Authentication (MFA)

4.1. All University members and third parties must enrol in University Multi-Factor Authentication (MFA) in order to protect their account.[4]

4.2. MFA protects user accounts and information by coupling a password with an additional factor – this includes, but is not limited to, smartphone authenticator app, One Time Password/Pin (OTP), SMS text code, and hardware token/key.

4.3. ICT shall provide guidance on enrolling MFA at support.hull.ac.uk.

[2] https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry
[3] https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers
[4] https://www.ncsc.gov.uk/blog-post/stepping-multi-factor-authentication