Password and Multi-Factor Authentication Policy

Document Reference: IT-POL-106

Document Classification: Policy

Data Classification: Public

Version number: 4.0

Relevant CIS Control(s): 5.2, 6.3, 6.4, 6.5

Status: Draft

Approved by (Board): University Leadership Team

Approval date: 25 September 2024

Effective from: 25 September 2024

Review Frequency: Annual

Next review date: 25 September 2025

Document author: Cyber Security

Document owner: Director of Technology

Contact: IT Services

Collaborative provision: No

State whether this document is applicable to the University's collaborative partners

Related documents: Information Security Controls Policy, User Account Policy, Password Manager Policy, Data Classification Policy.

University document: Yes

A University document applies across the institution, is approved by a committee of Council or Senate and is held in the University Policy Directory on SharePoint.

Published location: hull.ac.uk

- The University has adopted the principles of Designing for Diverse Learners, and all policy documents should be written with reference to these principles. Further information is available at the Designing for diverse learners website.
- An Equality Impact Assessment (EIA) must be considered for all new and amended policies. Further information is available from the EIA section of SharePoint.

Password and Multi-Factor Authentication Policy

1 Table of Contents

Password and Multi-Factor Authentication Policy

Introduction

1.1 This document outlines the Password and Multi-Factor Authentication (MFA) policy and guidance that 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 IT 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 IT Services systems and services such as email, cloud storage, and remote access, will be additionally protected by MFA.

1.4 Information systems owned by departments and faculties shall be protected by MFA where possible.

2 Scope

2.1 This policy, and all policies referenced herein, shall apply to all members of the University community, including faculty, students, administrators, staff, alumni, authorized guests, delegates, and independent contractors (the "End user(s)" or "you") who authenticate to the University's IT Resources.

2.2 This policy applies to all standard users.

2.3 Additional requirements for privileged users (e.g., administrators), and system specific accounts, are defined in the **User Account policy**.

3 Password Policy

3.1 The use of a password and MFA shall be required to access managed University-owned devices, including but not limited to laptops, desktops and servers.

3.2 All University members and third parties must set a unique password for all of their University accounts. Passwords should not be re-used across different accounts.

3.3 This password should not be used (or re-used) for any other services, whether personal or work/study related.

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

3.5 Passwords shall be at least 16 characters in length, although longer passwords or passphrases are recommended. There is no maximum password length.

3.6 Passwords will be subject to complexity requirements, for example the use of capital letters, numbers, and special characters.

3.7 Passwords will expire annually. This is to balance cyber security risks against the usability of creating and remembering a strong password.

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

3.9 Passwords must not be based on commonly used passwords. Where possible, technical controls should enforce this restriction.

3.10 Passphrases, including groups of random words are recommended as an alternative. Further guidance and examples can be found from the NCSC [1].

3.11 All University members and third parties must notify IT Services, if they know or suspect that their password has been compromised. They must change their password as soon as they can. Guidance on informing IT Services and changing their password can be found on the University website and the Support Portal.

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

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

3.14 Passwords should not be written down and left in an unsecure location (e.g., on desks, monitors, under keyboards). Doing so introduces the risk of university account compromise.

3.15 The use of password manager to generate and store credentials is encouraged and supported at the University. Popular password managers include KeePass, Bitwarden, and 1Password, however, users should be aware of the risks of doing so. Further guidance can be found from the NCSC[2].

[1] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
[2] https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers

3.16 Password guidance can be found on the Support Portal.

4 Multi-Factor Authentication (MFA) Policy

4.1 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.

4.2 All University members and third parties must enrol in University MFA to protect their University account[3].

4.3 MFA will be increasingly used across University IT systems as an additional method of authenticating University members. MFA implementation prevents unauthorised access to a University member's account, as well as the data they have access to.

4.4 University members should not share or disclose their MFA factor (including any one-time codes) with anyone else, including other colleagues/peers.

4.5 IT Services shall provide guidance on enrolling in and using MFA on the Support Portal.

4.6 Service owners must ensure that services they are responsible for have MFA capability. This should apply to new and existing services.

4.7 If a University member has any concerns about enrolling for MFA they need to contact IT Services in the first instance.

5 MFA and Data Classification

5.1 Figure 1, below, illustrates where MFA may be deployed based on the classification of information (see **Data Classification Policy**) as well as other factors, for example the device and network being used.

5.2 The model assumes that managed devices and trusted networks are, to some extent, inherently assured.

[3] https://www.ncsc.gov.uk/blog-post/stepping-multi-factor-authentication

5.3 The model also assumes that the risk of singular incidents such as device theft or network intrusion are high enough that MFA is still desirable where certain categories of information are accessible.

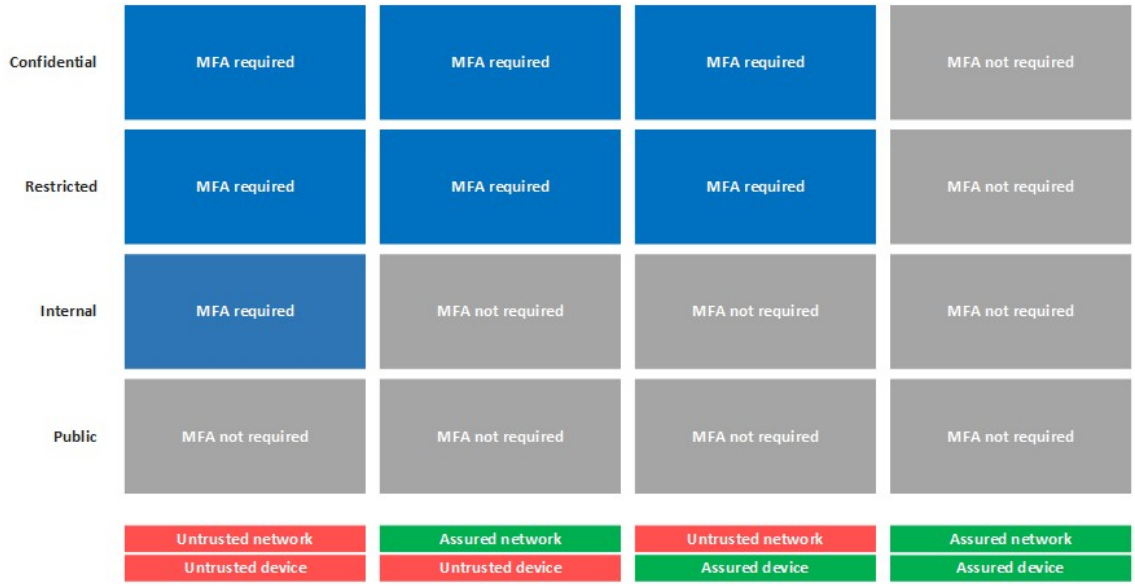

Figure 1: MFA Matrix based on Data Classification

6 Responsible, Accountable, Consulted, and Informed (RACI) Matrix

6.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[4]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[5]. A brief definition of each role is given in the table below.

6.2 The table below outlines the roles that are involved in ensuring this policy is adhered to, enforced, and kept up to date.

	Definition	Role
Responsible (R)	Answerable for the correct completion of the task	IT Services
Accountable (A)	Delegates and must sign off (approve) the work that those *responsible* provide	Director of Technology
Consulted (C)	Provide input based on how this will impact their domain of expertise	University Leadership Team
Informed (I)	Those who are kept up to date on progress	End Users

7 Version Control

Version	Author	Date approved	Relevant section(s)
1.0	Dan Chambers	19 April 2021	All
2.0	Steph Jones, Nigel Kavanagh	22 February 2022	All
3.0	Hollie Felice, Carl McCabe, Nigel Kavanagh	25 September 2023	All
4.0	Cyber Security		All

[4] https://www.forbes.com/uk/advisor/business/software/raci-chart/
[5] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/