Password and Multi-Factor Authentication Policy

Document Reference:	IT-POL-106
Document Classification:	Policy
Data Classification:	Public
Version number:	4.1
Relevant CIS Control(s):	5.2, 6.3, 6.4, 6.5
Status:	Approved
Approved by (Board):	University Leadership Team
Approval date:	03 June 2025
Effective from:	03 June 2025
Review Frequency:	Annual
Next review date:	03 June 2026
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

Table of Contents

Password and Multi-Factor Authentication Policy

1 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 from the requirements set out by the National Cyber Security Centre (NCSC).

1.2 All University IT systems use password authentication as a minimum. Recognising the limitations of passwords, core *IT Resources* such as email, cloud storage, and remote access, will be additionally protected by *MFA*.

1.3 A glossary of technical terms, which are defined in pink, underlined, and italicised, can be found at the end of this policy. Clicking on each term will take you to its definition.

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 IT Services Responsibilities

3.1 This section of the policy outlines the technical controls that IT services will be responsible for. These are applied in addition to the responsibilities of the end user, as described in section 4 and section 5.

3.2 Repeated password attempts will be subject to *throttling*.

3.3 User accounts will be locked after 10 unsuccessful password attempts.

3.4 *IT Resources* – namely end user devices – shall be configured to log out inactive end users after 15 minutes of inactivity.

3.5 When a new user account has been created, these will be required to change their password upon their first login.

3.6 When a new system, service, or device, for example, is implemented with a default password, IT Services shall change the default password upon first use.

3.7 Passwords shall not be transmitted over the network in clear text, or another readable format.

3.8 Passwords that are stored are to be strongly *encrypted*, to minimise unauthorised access to password data.

3.9 *MFA* will be required for university services, including but not limited to: those that are cloud-hosted, contain *protected information*, or are accessed by third-parties and/or privileged user accounts.

3.10 *Single-Sign-On (SSO)* is used where possible so that a user can authenticate seamlessly against multiple services.

4 Password Policy

4.1 The use of a password and *MFA* is required to access University *IT Resources*, including but not limited to laptops, desktops and servers.

4.2 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.

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

4.4 All end users 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.

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

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

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

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

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

4.10 *Passphrases*, including groups of random words, should be used wherever possible. Further guidance and examples can be found from the NCSC [1].

4.11 When entering a password, end users should be aware of their surroundings and ensure they are not being watched or filmed.

4.12 All end users 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.

4.13 If an end user suspects that a system has been compromised, they must report this to their line manager.

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

4.15 Passwords will be changed, and user accounts may be suspended, without notice when in response to a security incident or where IT Services monitoring detects suspicious activity.

4.16 Passwords must 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.

4.17 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].

4.18 Further password guidance can be found on the Support Portal.

[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

5 Multi-Factor Authentication (MFA) Policy

5.1 *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.

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

5.3 *MFA* will be 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.

5.4 End users should not share their *MFA* factor (including any one-time codes) with anyone else, including other colleagues/peers.

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

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

5.7 If an end user has any concerns about enrolling for *MFA* they should contact IT Services in the first instance.

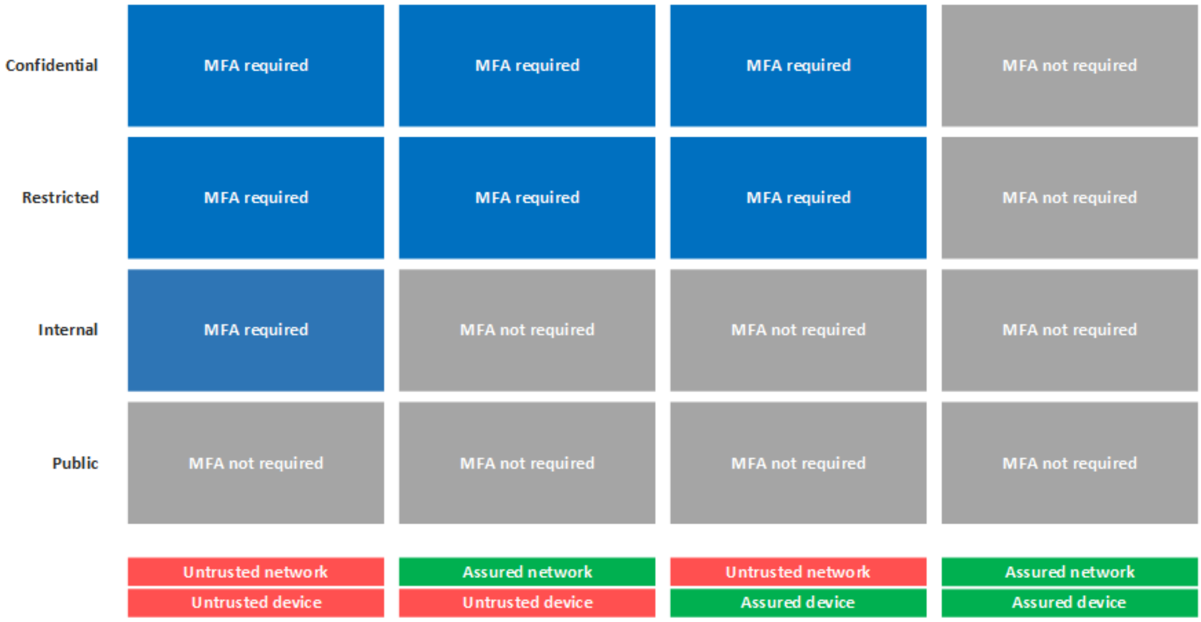
6 MFA and Data Classification

6.1 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.

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

6.3 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.

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



Confidential	MFA required	MFA required	MFA required	MFA not required
Restricted	MFA required	MFA required	MFA required	MFA not required
Internal	MFA required	MFA not required	MFA not required	MFA not required
Public	MFA not required	MFA not required	MFA not required	MFA not required
	Untrusted network	Assured network	Untrusted network	Assured network
	Untrusted device	Untrusted device	Assured device	Assured device

Figure 1: MFA Matrix based on Data Classification

7 Glossary of terms

7.1 *Encryption* = The process of encoding a message or information in such a way that only authorized parties can access it[4]. This provides an additional level of security, even greater than that of a password, by scrambling a file, for example, so that they cannot be opened unless correctly *decrypted*. This is similar to the use of a lock and key, where the use of a pseudo-random encryption key is generated by an algorithm. Encryption itself does not prevent interference but does hide the actual content of a file from a would-be interceptor.

7.1.1 *Decryption* = The process of using a 'key' to unscramble information. An authorized recipient, who possesses the key (encryption algorithm), can easily decrypt the message with the key provided by the originator5. It is theoretically possible to decrypt the message without possessing the key, but considerable computational resources and skills are required to 'crack'.

7.2 *IT resources* = Also known as an enterprise asset, these refer to a resource, owned by an enterprise (the University of Hull), with the potential to process or store data[6]. These include computing, networking, communications, application, and tele-communications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services. Figure 2, below, defines what is meant by an enterprise asset and provides examples – although it should be noted that this list is not exhaustive.

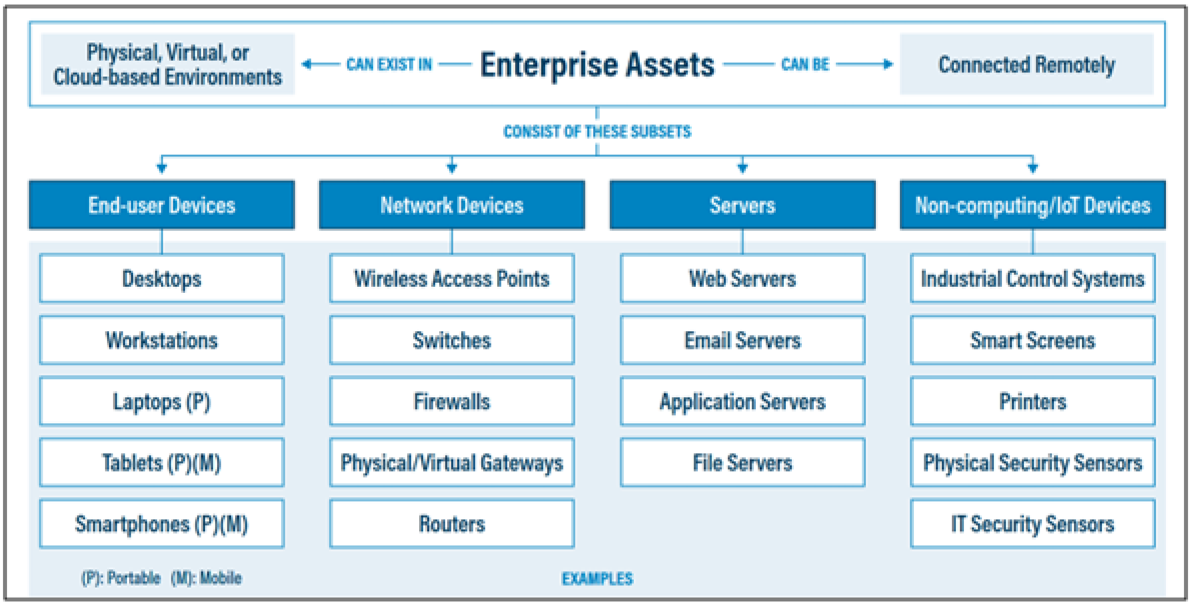


Figure 2: Enterprise Asset definition according to CIS Controls v8

7.3 *Multi-factor authentication (MFA)* = MFA is used to secure your access to university resources, to protect data from the increasing threat of cyber-crime. MFA is now widely used for access to sensitive information, and it's likely you've used a similar method for things like Internet Banking in the past. Most serious cyber-attacks are made possible using leaked or stolen account details. Even with our best efforts, it is still quite possible that someone knows your username and password, even if you've not shared them with another person. Your username and password are your *first* factor — something you *know*. We use tools provided by Microsoft to add a *second* factor to your account, which is usually something you *have*.

7.4 *Passphrase* = A type of password that is usually constructed from a string of words. In terms of security, the longer a password and/or passphrase is, the more difficult it is to 'crack'. However, the more random the words are to one another, the harder it is to guess; hence why it is important to avoid commonly used phrases or song lyrics. This is why the university follows the guidance from the National Cyber Security Centre (NCSC) and advises our users to 'Think Random' and use three random words[7].

1.1 *Password Manager* = A digital safe that store passwords. By knowing the password to the password manager, all stored credentials (usernames and passwords) can be accessed, and typically copied in or viewed, when needing to access an online account. This means that fewer passwords are needed to be remembered. Password managers can help prevent 'password fatigue', and password re-use, and can commonly also store other important information ranging from bank cards to Wi-Fi passwords. Most password managers have the capability to generate a strong password, or passphrase, too. It is imperative that a password manager is secured with a strong password or passphrase, as if this password is hacked or stolen, then unauthorised access to all the passwords stored in the manager are compromised too.

[4] https://www.cloudflare.com/learning/ssl/what-is-encryption/

[5] https://www.techtarget.com/searchsecurity/definition/cryptography

[6] CIS Controls Acceptable Use Policy Template (https://www.cisecurity.org/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls)

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

7.5 *Protected Information* = Information that comes under the **Data Protection Act** or **General Data Protection Regulations (GDPR)**, for example, or is sensitive (e.g., Personal Identifiable Information, PII, which can be used to associate with an individual) or confidential in some other way. Safeguarding the security of protected information is a complex issue, with organisational, technical, and human aspects. University policies and guidelines on Data Protection and Information Assurance are available on the University website.

7.6 *Single Sign-On (SSO)* = The process of using one set of credentials to access multiple separate resources[8]. This decreases 'password fatigue' by reducing the need for multiple individual sets of credentials, each with their own MFA requirements. As well as being used at the university, single sign-on (SSO) is a common option on websites, where you can sign in with Google, or a social media account.

7.7 *Throttling* = Password throttling is a mechanism that prevents passwords from repeatedly being entered incorrectly and progressively increasing the time delay between continuous login attempts[9].

[8] https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-single-sign-on

[9] https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

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

8.1 A form of a responsibility assignment matrix (RAM) commonly used in project management[10]. A RACI matrix defines who is involved in the successful completion / implementation of a project, task, or in this case, a policy[11]. A brief definition of each role is given in the table below.

8.2 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	Information Governance Committee
Informed (I)	Those who are kept up to date on progress	University Leadership Team

9 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	25 September 2024	All
4.1	Hollie Felice, Carl McCabe, Nigel Kavanagh	08 May 2025	All

[10] https://www.forbes.com/uk/advisor/business/software/raci-chart/

[11] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/