UNIVERSITY OF HULL

Password Policy

Classification:	Policy
Version Number:	1.0
Status:	Approved
Approved by (Board):	Information Governance Committee
Approval Date:	11 February 2020
Effective from:	11 February 2020
Next Review Date:	Annual
Document Authors:	Steph Jones, Security and Assurance Specialist, ICT
Document Owner:	Head of Service Assurance, ICT (Stewart Doyle)
Department/Contact:	support.hull.ac.uk
Summary:	This document outlines password policy and guidance for all University members
Scope:	All University members and third-parties required to authenticate with University ICT systems and services
Collaborative provision:	Not mandatory
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 Governance and Assurance Policy and Information Security Controls Policy at www.hull.ac.uk/policies
Published locations:	www.hull.ac.uk/policies
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 Policy

1. Introduction

1.1. This document outlines password policy and guidelines for all University members. This policy has been derived from the controls referenced by the Information Security Controls Policy and advice from the National Cyber Security Centre (NCSC).

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

1.3. This policy recognises the limitations of passwords and seek an effective balance between security and usability. Technical controls will be deployed where possible to overcome these limitations, including the additional layer of protection provided by Multi-Factor Authentication (MFA).

2. Scope

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

2.2. This policy applies to standard users. Additional requirements for privileged users and systems are defined in controls approved and managed by the ICT department.

3. Policy

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

3.2. All University members will protect their passwords 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 8 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]

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

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

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 in response to a security incident or where ICT monitoring detects suspicious activity.

3.11. University members are permitted to write their password down only if they are able to store and retrieve it securely – for example, in a locked drawer to which only they have access.

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

[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