Password Policy

Version 1.7

Version:	**1.7**
Dated:	**November 2019**
Document Owner:	**Head of IT Security and Compliance**

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
1.0	July 2017	I. Tilsed	New policy
1.3	Aug 2017	T. Dyhouse	Various small changes for latest Cyber Essentials certification
1.4	Sept 2017	I. Tilsed	Minor amendments
1.5	Oct 2017	P. Jones	CGR requested changes
1.6	April 2019	Ali Mitchell	Amended the minimum number of characters for password manager applications master passwords. Paragraph numbering added and changes to paragraphs 5
1.7	November 2019	Ali Mitchell	Paragraph 4 - removed and added in new links Improved layout and removed some characters used for programming.

Review Distribution

Version	Title	Date
1.7	Assistant Director Strategy and Architecture	November 2019
1.7	Assistant Director Service Management	November 2019
1.7	Chief Information and Digital Officer	November 2019
1.7	Operations and Security Manager	November 2019

Approval

Version	Position	Date
1.0	Members of the Information Security Group (ISG)	July 2017
1.7	IT SMT as minimal amendments	November 2019

Contents

1. Introduction

1.1 Passwords are an important aspect of computer security. Good password management will minimise the likelihood of user accounts being easily compromised, and mitigate risks to University information and IT systems. All users, including contractors and vendors with access to the University's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Scope

2.1 This policy applies to all individuals and groups with user accounts, with which to access the University's IT and network facilities. This includes, but is not limited to:

- staff (full-time, part-time and temporary)
- registered students
- consultants and contractors working for or on behalf of the University
- associates, visitor and conference delegates

It also applies to privileged accounts (used for managing IT systems and platforms).

3. Purpose

3.1 The purpose, or objective, of this policy is to establish the standard for the creation of strong passwords, the protection of those passwords and their ongoing management.

4. Related Policies and Documents

- Overarching Information Governance and Security Policy
- Data Breach Management Policy
- Regulations Relating to the Use of Information Technology Facilities
- Privacy and Personal Data Protection Policy
- Regulations Relating to the Use of Information Technology Facilities

5. Policy

5.1 All passwords must be treated as confidential information and must not be shared with anyone or made public in any form – written or verbal. They must not recorded (e.g. on paper, software file or hand-held device) unless this can be stored securely.

5.2 The use of keychains or password manager applications on devices including mobiles is permitted provided that these use:

- strong encryption to protect the stored passwords (e.g. Advanced Encryption Standard (AES) 256)
- 20 character passwords as a minimum to access the stored passwords
- multi-factor authentication

5.3 The same passwords must not be used for multiple University IT systems, where Single Sign On (SSO) is not in use. Users have the option to self-administer their own passwords by setting their security questions, for more details visit HERE.

5.4 University IT account details must not be used for non-University systems or applications, e.g. social media sites, retail websites, personal email and other such services.

5.5 Where a specific group of users require access to a particular system or service, they must be provided with their own unique login details to that system.

5.6 Privileged account users must ensure that their accounts use different and more complex passwords than their standard user accounts.

5.7 Users must change their password immediately if they suspect the details have been compromised and report it to the SID

6. Password Requirements

6.1 Complexity

Standard IT users are mandated to use passwords of at least 10 characters long; comprising of the 4 following types:

- Upper case letters
- Lower case letters
- Numbers
- Special characters, e.g. ! & , . = ‘ “ ; ? / { } [ ] ~ - \ ( ) _ + $ % ^ * @ #

Passwords must not contain the characters < : | or > as these are used in programming.

6.2 Use

- Passwords must not be shared with colleagues, for instance when on annual leave and IT staff will not ask users for details of their passwords. Applications, such as e-mail, often have delegated access, which must be used in these circumstances
- Passwords must be unique and must not be re-used
- Passwords must never be made public, for instance written on a note stuck to a workstation screen, or stored digitally in clear text
- Personal information must not be used as a password hint (e.g. the name of my dog) as it weakens the security of the account
- Avoid the use of ‘remember password’ features in applications
- Any suspected or actual incident or compromise relating to a password must be reported immediately to the SID, and the password changed as a matter or priority

6.3 Change

- All new IT users must change their password immediately after it has been used for the first login. Line managers, academic supervisors and guests sponsors must ensure they reinforce this as part of the new starter on boarding process.
- Changes to passwords must be in accordance with the complexity requirements defined in 5.1.

6.4 Anti-Brute Force Measures

6.4 Brute-force attacks are the automated guessing of large numbers of passwords until the correct one is found. For any internet-facing service, one of the following anti-brute force measures is used to protect against password guessing:

- lock accounts after no more than 5 unsuccessful attempts
- limit the number of guesses allowed in a specified time-period to no more than 5 guesses within 15 minutes

Such events will be logged.

7. Password Self-Reset Facility

It is mandatory that all users complete the information required for the password self-reset facility including the security questions. The Password self-reset facility and relevant information can be found HERE and on the University’s website at www.exeter.ac.uk

8. Compliance and Enforcement

The University has an obligation to comply with various statutory, legal and contractual requirements. This policy forms part of the wider information governance and security suite of policies and good practice, designed to ensure user account details are managed effectively to mitigate any risks to the integrity, availability and confidentiality of University information and IT systems.

Relevant disciplinary procedures will be used in cases where a student or staff member fails to adhere to this policy.

Commercial contracts for third parties and contractors must contain clauses referring to this policy and the consequences of non-conformance.

Any exception to the Password Policy must be approved, in advance, by the Chief Information and Digital Officer, or nominated deputy.

9. Help and Advice

For any issues relating to resetting your passwords please contact the SID on 0300 555 0444 or extension 4724. For any comments regarding this policy please email the IT Security and Compliance team itsecurityandcompliance@exeter.ac.uk