IGSSG24 16-17

Exeter IT

Password Policy

Document Control Information:

Date:	26/05/17
Master Tracking Name	Password Policy
Master Tracking Reference	
Owning Service / Department	Exeter IT
Issue:	v.1.0

Approvals:

Author:	Assistant Director, IT (Strategy & Architecture)
Approved By:	Exeter IT Senior Management Team
Authorised By:	Chief Information & Digital Officer
Approving Body:	Information Governance and Security Steering Group (IGSSG)

1 Introduction

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 Purpose

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.

3 Scope

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 services).

4 Principles

All passwords must be treated as confidential information and should not be shared with anyone or made public in any form – written or verbal.

Passwords must not be recorded (e.g. paper, software file or hand-held device) unless this can be stored securely. Use of keychains or password manager applications on mobile devices and computers is permitted provided that these use:

- strong encryption to protect the stored passwords (e.g. AES-256)
- a strong 14-character password to access the stored passwords.

The same passwords must not be used for multiple University IT systems, where Single Sign On (SSO) is not available and users have the option to set their own passwords.

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.

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.

Privileged account users must ensure that their accounts are different from their standard user accounts, and different for each system or service.

Passwords and the systems implementing them must follow the technical standards set out in a separate technical document.

5 Password Requirements

5.1 Complexity

Passwords should be at least 10 characters long. This is the baseline for all University accounts. Advice on the generation of strong passwords is set out in a separate document.

Passwords should not contain the characters < > : ¦ and a space as these are used in programming.

5.2 Use

Passwords should not be shared with colleagues, for instance when on annual leave. Applications, such as e-mail, often have delegated access, which should be used in these circumstances.

Passwords should be unique and should not be re-used.

Passwords should never be made public, for instance written on a note stuck to a workstation screen, or stored digitally in clear text.

Personal information should 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 should be reported immediately to SID, and the password changed as a matter or priority.

5.3 Change

The initial or default password provided when connecting to a network, application or other system for the first time should be changed. This is particularly important when a new student or member off staff is provided with an account on joining the University.

Whilst regular change is not mandated, if a password has been used with another account, or it is suspected that someone has knowledge of the current password, then the creation of a new password is strongly recommended.

Changes to passwords should be in accordance with the complexity requirements defined in 5.1 and associated documents.

5.4 Reset

Any process for the resetting of passwords should confirm the requester's identity before any password is reset.

6 Compliance & 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 should 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.

7 Policy Review and Maintenance

The Password Policy will be reviewed and updated, annually, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.
