PASSWORD POLICY

1. Introduction

Technical, physical, and administrative controls are applied across the University's IT infrastructure to protect our facilities and data from unauthorized access. Provision is however made for legitimate users to access systems and data relevant to their roles when and where it is required via user accounts and passwords. To provide accountability and prevent abuse of user accounts, it is imperative that users use strong passwords and manage them in a secure manner. Doing so will help prevent unauthorized access to systems and preserve the confidentiality, integrity and availability of data.

This document forms the Password Policy and defines the password controls that are designed to protect University of Reading users, systems, and data.

2. Scope

This policy applies to the below users authenticating to University of Reading IT systems:

- All employees working for or on behalf of the University.
- All registered students of the University.
- All consultants and contractors working for or on behalf of the University including third party companies that work remotely to access our systems.
- Individuals who have been granted access to the University's IT and network, including visitors.

3. Roles and Responsibility

3.1 All users of University of Reading IT systems shall:

- Read, understand and comply with this and other related policies.
- Choose sensible and strong passwords at all times. The University will not necessarily configure systems to enforce strong passwords but this does not excuse users from choosing weak passwords.
    - For guidance on choosing a strong password, visit the University's cyber security webpages:

      https://www.reading.ac.uk/internal/its/cybersecurity/passwords.aspx
- Ensure the secrecy of their passwords and control access to their user accounts through password security.
- Not divulge their passwords to anyone (including system administrators, security staff and management).
- Change default or reset passwords themselves if systems cannot be configured to force change them upon first logon.

- Will, if there is any indication that an account has been compromised, change their password immediately and report it as an incident to the IT Service Desk.

3.2 The Information Security Team shall:

- Periodically review user passwords to ensure they meet the minimum requirements as specified in this policy.
- Investigate:
  - Multiple failed login attempts.
  - Login attempts from unexpected geographical areas.
  - Reports of unexpected account lockouts or other unusual account behaviour from users.
  - Compromised accounts.
- Ensure that advice and guidance on password management is made available to staff and students.

3.3 IT Administrators shall:

- Implement a process (where possible) that force changes the password for newly created accounts at first log on.
- Ensure that password settings are changed immediately from their default settings.

3.4 The University's Policy Group are responsible for the implementation, monitoring and review of this policy.

4. Requirements and Key Principles

4.1 To create a strong password, the single most important factor is password length (assuming the password isn't easily guessable by other means e.g. repeating characters, username, etc.).

4.2 Consider using biometrics (where possible) and passphrases e.g. 1Likebigboots!

4.3 Multi-factor authentication shall be used where possible (and appropriate) for all important accounts and internet facing systems.

4.4 Where access is shared (e.g. mailboxes, shared network drive/folders), access is controlled in accordance with the *Access Control Policy*.

4.5 The *Privileged Account Management Policy* details the password guidelines for privileged accounts.

Password Creation

4.6 The following password criteria (as a minimum) must be met:

- Must be a minimum of 12 characters in length (longer is better).
- Must not contain your username.
- Should not contain repetitive or sequential characters e.g. 'aaaa' or '1234'
- Should not be a recycled password or recycled with the addition of a character e.g. Password1 to Password2.
- Users shall ensure that different passwords are allocated and used across different systems and accounts.

4.7 A good way to create a strong and memorable password is to use a passphrase or three random words e.g. 'CoffeeTrainFish29' and '8RedHouseMonkeys'.

Password Manager/Vault

4.8 Consider using a password manager (LastPass, KeePass, 1Password) to generate and store passwords. The typical user has dozens of passwords to remember. To cope with this overload, users often resort to insecure workarounds (such as password reuse or using common passwords) which are more open to being exploited by attackers. Password managers offer an alternative, more secure, way of coping with password overload.

5. Related policies, procedures, guidelines & regulations

This policy sits beneath the University of Reading's overarching *Information Security Policy*. This and other supporting policies can be found here:

http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
1.0	N/A	DTS	Biennially	University Policy Group	May 20	May 20	May 22