University of Reading

Digital Technology Services (DTS)

Password Policy

1. Purpose

All users have the responsibility for the activity of their designated IT accounts and must not share logon credentials with other individuals as stated in the University's IT User Regulations. In order to ensure confidentiality, integrity, and availability of the University's resources, users must follow the guidance set out in this policy to protect and maintain the security of their passwords.

2. Scope

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

- Employees (including temporary or short term workers) of the University or a subsidiary company of the University.
- All registered students of the University.
- Contractors engaged by the University.
- Volunteers, interns and those undertaking placements or work experience.
- Those with University accounts by virtue of a visiting or courtesy title conferred by the University.

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 passwords that comply with this policy.
  - For guidance on how to comply with this policy visit the University's cyber security webpages: Passwords (reading.ac.uk).
- Not divulge their passwords to anyone (including system administrators, security staff and management, friends and family).
- Change default or reset passwords themselves, if systems cannot be configured to force the change upon first logon.
- Not reuse the password for any other IT account whether at the University or for personal use.
- Enrol in the University Multi-Factor Authentication (MFA) system, to protect their account.
- If there is any indication or evidence that an account has been compromised, change their password immediately and contact DTS service desk to report the incident, and for assistance to change the password when required.

3.2 The Information Security Team shall:

- Periodically review information systems configuration settings for conformance to this policy.
- Reserve the right to 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 Systems Administrators and Business Systems Owners shall:

- Ensure the secrecy of their passwords and control access to their user accounts through Identity Management Systems where technically possible.
- Implement a process, where technically possible, that forcefully changes the password for newly created accounts at first log on and for newly reset passwords on existing accounts.
- Ensure that password settings are changed immediately from their default setting.
- Log privileged account password resets at the system level and hold these for a minimum of 180 days.

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

4. Requirements and Key Principles

4.1 To create a strong password, the single most important factor is password length (consider using a passphrase or three random words).
4.2 Consider using biometrics as another layer (where possible) and passphrases.
4.3 Multi-factor authentication shall be used where the system supports it for all accounts on SaaS platforms, externally hosted and internet facing systems.
4.4 Passwords should not be shared via insecure transport mechanism or in clear text.

Password Creation

4.5 The following password criteria (as a minimum) should be met:

- Must be a minimum of 12 characters in length (longer is better).
- Must not contain username, surname and/or given name or other personally identifiable information of the user.
- Must contain at least 1 of each of the following: Uppercase letter, lowercase letter, a number and special character
- Should not contain repetitive or sequential characters e.g. 'aaaa' 'abc' or '1234'
- Should not be a recycled password or recycled with the addition of a character e.g. Password1 to Password2.
- Users must ensure passwords must be unique and not have been previously used by them on any IT account.
- Passwords should never be stored in clear text on paper, or in non-protected files.
- Privilege and Service accounts should have a minimum password length of 16.

4.6 See Passwords (reading.ac.uk) for guidance on password creation techniques.

Password Manager/Vault

4.7 Consider using a password manager 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. Note, do not store University account credentials in a private password manager and vice-versa.

5. Consequences of Non Compliance

Failure to comply with this policy may result in revocation of your access to the University's systems, whether through a device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, worker or volunteer, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether or not the breach takes place at your normal place of work.

6. Related policies, procedures, guidelines or regulations

This policy sits beneath the University of Reading's overarching *Information Security Policy*. This and other supporting policies (including "IT User Regulations") can be found on the Information Compliance Policies (reading.ac.uk) page.

Document control

Version	Keeper	Reviewed	Approving authority	Approval date	Start date	Next review
1.0	DTS	Biennially	University Policy Group	May 20	May 22	May 24
1.1	DTS	Biennially	University Policy Group	June 24	Aug 24	Jun 27