Cardiff University IT Systems Password Policy

Version Number	1.3
Document Status	Approved
Date Approved	15 January 2019
Approved By	Data and Information Management Oversight Group
Effective Date	15 January 2019
Date of Next Review	January 2021

1. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Policy Statement

The University shall ensure that its information assets are appropriately protected by passwords where necessary and that those passwords are technically secure and kept securely.

3. Scope

3.1 The scope of this policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Cardiff University facility, has access to the Cardiff University network, or stores any non-public Cardiff University information. This includes all computer systems, including laptops, personal digital assistants (PDAs) and smart phones.

3.2 The use of digital certificates for authentication is not covered by this policy.

3.3 Where systems cannot support the required password complexity please see section 7. below.

4. Relationship with existing policies

This policy forms part of the Information Security Management Framework

This policy should be read in conjunction with the following regulations and policies:

- University IT Regulations
- University Acceptable Use Policy
- University IT Security Policy
- Guidelines on Personal Use of Cardiff University IT Systems

5. Policy Objectives

5.1 Where information assets require protection on the basis of confidentiality, integrity or availability passwords shall be required to access those systems that contain the assets.

5.2 Passwords and the system implementing them shall follow the technical standards set out below.

- All passwords for accessing Cardiff University systems are to be classified as highly confidential information.
- Once communicated to the original user, passwords shall not be shared or revealed to another person. Where third party access to an account is required for business purposes a request for assistance should be made via the IT Service Desk and a formal process for changing the password will be applied if necessary.
- Passwords must not be stored insecurely.
- If an account or password compromise is suspected, report the incident to IT Services or the system administrator immediately.

6. Technical Standards

6.1 Computer System Administrators

6.1.1 Password length shall be a minimum of 10 characters.

6.1.2 Passwords shall include a mixture of upper and lowercase characters.

6.1.3 Passwords shall contain at least one number

6.1.4 System-level (root, administrator) passwords shall include at least one special character.

6.1.5 A setting shall be enabled to prevent the use of commonly used passwords e.g. Password01.

6.1.6 Sharing of System-level (root, administrator) accounts shall not be used. Administrators shall each have a unique username and password.

6.1.7 Password history shall be enabled to prevent re-use of passwords within 12 months.

6.1.8 Where a system provides either Intruder lockout or break-in evasion features one of these features shall be enabled. For intruder lockout it is recommended accounts are locked following 3 consecutive login failures.

6.1.9 Passwords shall not be stored in plain, unencrypted, form. If possible asymmetric cryptography shall be used. Password files or databases must be protected to prevent unauthorised access or copying.

6.1.10 For disaster recovery one written copy of system passwords may be held in a secure location for example a departmental/school safe or a password vault such as a KeePass (http://keepass.info/) may be used.

6.1.11 Compromise, due for example to interception, of the password during distribution to users must be managed. Please refer to IT Services Guidance on Distribution of Initial Passwords to Users.

6.1.12 Instructions on how to reset passwords must be made available to users by system administrators.

6.1.13 Where SNMP is used, the community strings must be defined as something other than the standard defaults of “public,” “private” and “system” and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g. SNMPv2).

6.1.14 Use of embedded passwords in programme scripts or configurations files is not recommended. Where there is no alternative method, access to the script or configuration files must be controlled to prevent unauthorised disclosure of passwords. Accesses shall be monitored or logged to detect unauthorised access.

6.1.15 User accounts that have system-level privileges granted through group memberships or programs such as “sudo” must have a unique password from all other accounts held by that user.

6.2 Application Development Standards

6.2.1 Application developers must ensure their programs contain the following security precautions.

Applications:

a) Shall support authentication of individual users, not groups.

b) Shall not store passwords in clear text or in any easily reversible form.

c) Shall provide for a form of role management, such that one user can take over the functions of another without having to know the other's password.

d) Shall support RADIUS and/or X.509 with LDAP security retrieval wherever possible.

7. Transitional Arrangements

7.1 Systems which cannot meet the criteria shall, following appropriate risk assessment of the information being protected by the password, fall into 3 categories

7.1.1 They represent a low risk to the University even if the password was compromised and so are exempt from the password policy (e.g. the password to log onto a microscope in a lab)

7.1.2 They are a moderate risk and so are exempt for a set period or until the next major release based on that release adding support for the above password requirements,

7.1.3 They represent a high risk (e.g. contain classified data) and are exempt for a period (determined by the level of risk) while alternative provision is sourced or until a procedural measure can be introduced to add an extra layer of security, mitigating the risk – e.g. the system is only accessible from a room which is protected by swipe card access.

8. Responsibilities

8.1 All users

- have a responsibility for the security of their own passwords and for reporting a potential disclosure of their own or any other users' passwords.

8.2 System administrators

- must ensure the systems they have responsibility for, implement this password policy.

8.3 System Purchasers

8.3.1 This policy must be taken in to consideration when specifying and selecting or designing new computer systems and software.

9. Compliance

9.1 Breaches of the University IT Systems Password Policy may be treated as a disciplinary matter dealt with under the University's staff disciplinary policies or the Student Disciplinary Code as appropriate.