Password Policy for IT Systems

Information Services

Passwords are an important aspect of computer security and the failure to use strong passwords may lead to the compromises of information and information systems.

1. Purpose

This policy establishes 1) a minimum standard for the creation of strong passwords, 2) the protection of those passwords, and 3) the frequency of change of University passwords.

2. Scope

This policy applies to any person registered to use services on the Cranfield University IT network and includes students, staff, third party contractors, and any other affiliated personnel.

3. Policy

When creating strong passwords users need to ensure that they:

- are a minimum of 8* characters (with no set maximum)
- do not contain the user's account name
- do not use common passwords e.g. "Cranfield!" or "Pa55word"
- do not use easily discoverable information such as name of favourite sports team
- do not contain 2 consecutive characters of the user's full name
- do not use the same password anywhere else – Your University password must be unique
- contain a mix of characters from 3 of the following 4 categories:
    - uppercase letters (A-Z)
    - lowercase letters (a-z)
    - numbers (0-9)
    - special characters (for example, !, $, @, %)
- are changed at least every 12[#] months, or immediately if you believe they have been compromised or become known
- do not contain common words found in a dictionary (see Network Password Guidelines for tips on using passphrases)
- are not shared or disclosed

* Mobile devices such as smartphones/tablets/laptops must use access controls, be a minimum of 6 characters (which can be further strengthened by the use of pattern-matching or biometric authentication controls) and follow the above complexity rules, where possible.

[#] Access controls for mobile devices (i.e. not passwords) do not need to be changed every 12 months but must be changed if the device or control has been compromised (i.e. lost or stolen).

4. Security controls

To protect against 'brute-force' attacks all internet-facing services will have lock-out mechanisms to deter repeated attempts to guess account details. These mechanisms will ensure that the account is temporarily suspended under such conditions.

All University IT systems will be configured to ensure that passwords can only be transmitted in an encrypted format to reduce the risk of compromise via interception.

Any passwords stored by the University will be in an encrypted format that includes 'password salting[1]' to ensure that actual passwords cannot be recovered from the stored hashes.

The IT Service Desk will never ask for full details of your password or other security credentials (unless you have self-initiated a password reset with the Service Desk), and therefore you should never provide these either over the phone or in an email message. Further information on how to select and remember 'strong' passwords can be found in the Network Passwords Guidelines document.

If you need to physically record a password then this should be stored in a suitably secure location e.g. sealed envelope in a secure cupboard/drawer.

In addition, the use of commercial password management applications can be used where users have a need to record a large number of passwords and further advice can be sought from IT Security (ITsecurity@cranfield.ac.uk).

5. Password Manager

The University's Password Manager service can be found on the internet here:

www.cranfield.ac.uk/pwman

It can be used anywhere in the world to change your password, review your security questions and answers, inform you of when your password is set to expire and unlock your University IT account.

[1] National Cyber Security Centre's Password Guidance (Tip 7): https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Document control

Document title	Network Password Policy for IT Systems
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Services
Approval by and date	Director of Information Services; 14/11/2018
Date of last review and version number	November 2018; V1.3
Date of next review	August 2019
Information categorisation	Open

Document Review

Version	Amendment	By	Date
1.1	New branding applied	Information Security Specialist	November 2016
1.2	Minor revisions to bring the policy in-line with National Cyber Security Centre recommendations	Information Security Specialist	January 2018
1.3	Changes to Section 4	Information Security	November 2018