Password policy and guidance for Information Technology (IT) systems

Information Technology

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

1. Purpose

This policy establishes a minimum standard for the creation and use of password, which are used in conjunction with multi-factor authentication to validate access to IT systems and services.

2. Scope

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

3. Policy

When creating strong passwords users need to ensure that they:

- use a unique password for their University account – i.e. it must not be used to access any non-University systems or services
- use 3 randomly selected words[1] and add numbers or special characters
- are a minimum of 8* characters (with no set maximum) for standard user accounts
- are a minimum of 15 characters for Admin accounts
- 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
- 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 immediately if you believe they have been compromised or become known
- do not contain common words found in a dictionary
- 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.

[1] https://www.youtube.com/watch?v=1bkYxRXF1aw

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' 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

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 management

Passwords should always have a meaning and be difficult to guess but easy to remember. As they are valuable, they should always be kept safe from prying eyes!

When choosing passwords, to meet the length and complexity rules you could try using the following methods:

- use 3 randomly selected words[2] "photo", "bottle", "poppy" then add numbers or special characters to form "6photobottlEpoPPy6!?"
- use the first letter of each word in a memorable phrase, saying, nursery rhyme or song title e.g. "Do you know the way to San Jose" becomes dyKtw2SJ?
- use an ordinary word or phrase and change, delete, or add characters so that it becomes nonsensical e.g., Cranfield = £r@n5ielD
- try typing entire passphrases, such as "Wonderful weather today" but substituting some letters with numbers and special characters e.g. "Wond3rfulwe@thertoday?"

If you suspect that your account has been compromised, or abused, or is always 'locked' out when you want to use it please notify the IT Service Desk, and change it immediately.

6. Resetting your password

If you have forgotten your password or have been locked out of your account, you can use your Microsoft account security info and mobile phone/personal email address to create a new one.

Note: You must have at least two methods of authentication in place for the password reset tool to work. If you don't already have this in place, please contact the IT Service desk.

Follow the instructions in IT26_Changing_your_password and use: https://passwordreset.microsoftonline.com/.

[2] https://www.youtube.com/watch?v=1bkYxRXF1aw

Document control

Document title	Password policy and guidance for IT Systems
Document number	CU-IT-POL-4.01
Originator name/document owner	Information Security
Professional Service Unit/Department	Information Services
Approval by and date	Information Assurance Committee; 25/09/2023
Date of last review and version number	October 2023; V1.8
Date of next review	August 2024
Information categorisation	Open

Document Review

Version	Amendment	By	Date
1.8	Annual review	Information Security	October 2023