Network Password Policy for Information Technology (IT) Systems

Information Services (IT)

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 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
- 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 should have access controls activated but these may be a minimum of 6 characters (or an equivalent pattern-matching/biometric strength) and do not need to adhere to the above complexity rules.
Passwords/PIN’s used to access mobile devices (smartphones/tablets) do not need to be changed every 12 months but must be changed if the device or password has been compromised.

4. Guidelines

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.
# Document control

<table>
<thead>
<tr>
<th>Document title</th>
<th>Network Password Policy for IT Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator name/document owner</td>
<td>Information Security Specialist</td>
</tr>
<tr>
<td>Professional Service Unit/Department</td>
<td>Information Services</td>
</tr>
<tr>
<td>Implementation/effective date</td>
<td>2009</td>
</tr>
<tr>
<td>Approval by and date</td>
<td>Director of Information Services; 18/01/2018</td>
</tr>
<tr>
<td>Date of last review and version number</td>
<td>January 2018</td>
</tr>
<tr>
<td>Date of next review</td>
<td>August 2018</td>
</tr>
</tbody>
</table>

## Document Review

<table>
<thead>
<tr>
<th>Version</th>
<th>Amendment</th>
<th>By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>New branding applied</td>
<td>Information Security Specialist</td>
<td>November 2016</td>
</tr>
<tr>
<td>1.2</td>
<td>Minor revisions to bring the policy in-line with National Cyber Security Centre recommendations</td>
<td>Information Security Specialist</td>
<td>January 2018</td>
</tr>
</tbody>
</table>