

PASSWORD STANDARD

The purpose of this document is to outline Aberdeen City Council's minimum requirements for the creation of strong passwords.

This Standard is to be used in conjunction with the ICT Access Control Policy, which outlines the Council's rules for password creation and management.

Workstations, Systems and Applications

The minimum requirements for workstation, system and application user account passwords that are changed or created are that they:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least 8 characters in length
- Contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters (e.g., !, \$, #, %)
- Do not repeat the last 5 passwords used

Administrator Accounts

The minimum requirements for system and application administrator accounts is that they:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least 15 characters in length
- Contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters (e.g., !, \$, #, %)
- Do not repeat the last 5 passwords used

Mobile Devices

The minimum requirements for Council mobile device passwords are that they:

- Be at least 8 alphanumeric characters long
- Repeat a character no more than 3 times
- Have no more than 3 numbers in a row
- Be changed after a maximum of 90 days
- Do not repeat the last 2 passwords used

Using a fingerprint to secure a Council mobile device is allowed in addition to the device password. However, if the device hasn't been used for 24 hours, or if the device has been restarted, the password will be required to unlock it.