Password Policy

Purpose of the policy

It is good practice to enforce a password policy, which ensures that passwords are difficult to crack. This increases the security of our systems and the information held by them.

The password policy determines the settings for passwords, such as how long passwords last before they expire. This policy will be enforced automatically when logging on to the network through Windows.

1. Enforce password history

This security setting ensures that several previous passwords are remembered. This means that users cannot use the same password when their password expires. The setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused.

The value is set to 20. This means that you can’t re-use an old password until you have used 19 other, different passwords.

2. Maximum password age

This security setting determines the period of time (in days) that a password can be used before the system requires the user to change it.

Security best practice dictates that passwords expire every 30 to 90 days, depending on the environment. This way, an attacker has a limited amount of time in which to crack a user's password and have access to network resources.

Passwords will be set to expire after 42 days, which is the default.

3. Minimum password age

This security setting ensures that passwords cannot be changed until they are more than a certain number of days old. Staff must wait the specified number of days (or longer) to change their passwords.

Without a minimum password age, staff could cycle through passwords repeatedly until they get to an old favourite.

The minimum password age is set to 7 day. This means that, after you change your password, at least a day must pass before you can change it again.

4. Minimum password length

Long passwords, of eight or more characters, are usually stronger than short ones. With this policy setting, users cannot use blank passwords, and they have to create passwords that are a certain number of characters long.

Passwords must be at least eight characters long, which is the default.

The length of the password is not limited and so the use of a ‘passphrase’ is recommended, a ‘passphrase’ is when a short sentence is used as a password. They are more secure because they are made up of multiple words separated by spaces. When using a passphrase please follow some simple guidance:

- It should be long enough to be hard to guess
- It should not be a famous quotation from literature, holy books, etc.
- It should be hard to guess by intuition even by someone who knows you well

It should be easy to remember and for you to type accurately.

5. Passwords must meet complexity requirements

This policy setting checks all new passwords to ensure that they meet basic strong password requirements. Passwords must:

- not contain all or part of the user's account name
- be at least eight characters in length
- contain characters from two 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 (for example, !, $, #, %)

Complexity requirements are enforced when passwords are changed or created.

Note that you can use numbers but still have memorable passwords. For example, if your password would be ‘penrith’ you could make it stronger like this: ‘P3nr1th’ with a 3 for the e and a 1 for the I, with a capital letter at the start.

Passwords that will comply with this policy

At first, your main Windows logon will be the only password that will have to comply with this policy. However, over time, all systems that can enforce passwords that comply with the policy will follow suit.