Corporate Policy for Account Password Settings

1. Introduction

Users often have many different computer accounts at work, at home, for their mobile phone, at their bank, with insurance companies, and so on. To make it easier to remember their passwords, users often use the same or similar passwords on each system; and given a choice, most users will select a very simple and easy-to-remember password such as their birthday, their mother's maiden name, or the name of a relative. Short and simple passwords are relatively easy for attackers to determine. Some common methods that attackers use for discovering a victim's password include:

- Guessing—The attacker attempts to log on using the user's account by repeatedly guessing likely words and phrases such as their children's names, their city of birth, and local sports teams.
- Online Dictionary Attack—The attacker uses an automated program that includes a text file of words. The program repeatedly attempts to log on to the target system using a different word from the text file on each try.
- Offline Dictionary Attack—Similar to the online dictionary attack, the attacker gets a copy of the file where the hashed or encrypted copy of user accounts and passwords are stored and uses an automated program to determine what the password is for each account. This type of attack can be completed very quickly once the attacker has managed to get a copy of the password file.
- Offline Brute Force Attack—This is a variation of the dictionary attacks, but it is designed to determine passwords that may not be included in the text file used in those attacks. Although a brute force attack can be attempted online, due to network bandwidth and latency they are usually undertaken offline using a copy of the target system's password file. In a brute force attack the attacker uses an automated program that generates hashes or encrypted values for all possible passwords and compares them to the values in the password file.

Each of these attack methods can be slowed down significantly or even defeated through the use of strong passwords.

The Account Password Settings Policy aims to promote the use of strong passwords for Council Network Access.

2. Objectives of the Policy

The objectives of the policy are to manage security settings in relation to authentication and log on to the Authority's Network through the consistent application of the following password characteristics:

Enforce password history,

Maximum password age,

Minimum password age,

Minimum password length,

Passwords must meet complexity requirements

3. Scope of the Policy

This policy affects all users accessing the Authorities Network - both internal and external. More specifically this includes

- All Staff accessing the internet
- All Third Party Contractors and Support
- Home / Remote Workers

4. Policy

Enforce password history: This determines the number of unique new passwords a user must use before an old password can be reused.

This value is set at 24 passwords

Maximum password age: This determines how many days a password can be used before the user is required to change it.

This value is set at 56 days.

Minimum password age: This determines how many days a new password must be kept before the user can change it. This setting is designed to work with the **Enforce password history** setting so that users cannot quickly reset their passwords the required number of times, and then change back to their old passwords.

This value is set at 2 days.

Minimum password length: This determines the minimum number of characters a password can have.

This value is set to 8 characters.

Passwords must meet complexity requirements: This determines whether password complexity is enforced. These complexity requirements are enforced upon password creation and ensures user passwords meet the following requirements:

- The password is at least eight characters long.
- The password contains characters from at least three of the following five categories:

Group	Example
Lowercase letters	a, b, c, ...
Uppercase letters	A, B, C, ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9

Group	Example
Non-alphanumeric (symbols)	( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /
Unicode characters	€, Γ, ƒ, and λ

- The password does not contain three or more characters from the user's account name.

  (When checking against the user's full name, several characters are treated as delimiters that separate the name into individual tokens: commas, periods, dashes/hyphens, underscores, spaces, pound-signs, and tabs. For each token that is three or more characters long, that token is searched for in the password; if it is present, the password change is rejected. For example, the name "Erin M. Hagens" would be split into three tokens: "Erin", "M", and "Hagens". Because the second token is only one character long, it would be ignored. Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password. All of these checks are case-insensitive.)

Account Lock out: This determines how many attempts the user will have to successfully log onto the network before the Account is locked and can only be reset by an administrator.

This value is set to 3 attempts.

Account Lock out duration: This determines the length of time a lock out is applied.

Reset automatically after 30 mins,

Bad Password Count: This determines the length of time password attempts are counted.

Reset automatically after 30 mins,