GENEVA COLLEGE INFORMATION TECHNOLOGY SERVICES

Password POLICY

Table of Contents

OVERVIEW

Geneva Information Technology Services hosts a vast array of data systems and technologies, many of which require reusable passwords as the most basic form of authentication. This requires that minimum standards be set, providing a framework of acceptable security across all systems.

The following outlined policy does not prevent the use of more stringent password requirements, such as the use of longer passwords or greater complexity requirements. It is however, intended to provide a minimum acceptable level of strength and complexity to protect the end users' passwords against attack.

In cases where password requirements cannot be met (password complexity, password expiration), further augmentation of the processes around that authentication must be made, such as upgrades or hotfixes to support more stringent requirements, or a stronger form of authentication such as 2-factor authentication must be adopted.

PURPOSE

This document addresses end users' passwords and not the strength of administrators' passwords, which should be significantly more complex and provide additional security against attack. The purpose of this policy is to define standards for password length, complexity, expiration, lockout, age, history and use.

SCOPE

This policy applies to the following Geneva user accounts:

- Computer (Windows) Accounts
- Email accounts
- Student Information System Accounts (EX, PowerFAIDS, JRM, etc.)
- myGeneva Accounts

DEFINITIONS

1. Length - The minimum number of characters required. Historically, passwords of greater length have been seen as more difficult to crack.
2. Complexity - The minimum number of characters from an alphanumeric (A-Z, 0-1), non-alphanumeric (#$%_), Unicode and upper and lower case which must be included in a password. Some consider complexity more important than password age, since cracking a complex password can be measured in weeks or months. Dictionary passwords that can be broken in minutes are not aided by expiration that is measured in weeks. Note: In some cases, the complexity also prevents the password from containing any pattern of characters taken from the account's user name.
3. Expiration - The amount of time before a password must be changed. Password age can be insignificant if the password is not sufficiently complex.
4. Account Lockout - The number of times a password can be incorrectly attempted before locking the account. This setting is critical, especially in the case of more complex passwords. By leveraging Rainbow Tables, an attacker can try all possible combinations of characters to crack a password. If no lockout exists, the attacker can try indefinitely. It must be set to allow a normal user to make a few mistakes in entering their password. Note: Account lockout, when set, can lead to Denial of Service (DoS) attacks against an authentication system. This would prevent authorized users from being able to authenticate.

5. Account Lockout Reset - The amount of time a user must wait before the system unlocks their account automatically. This prevents many calls to the Help Desk by legitimate users which might have recently changed their password or have the Caps Lock key inadvertently pressed. Note: In some cases, environments have chosen to not allow the system to automatically reset passwords. This is not considered more complex than having it performed automatically, but may increase communication to end users the importance of remembering their password.
6. Minimum Password Age - This security setting determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days, or you can allow changes immediately by setting the number of days to 0. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite.
7. Password History - This setting defines the number of passwords remembered by the system. This prevents a user from setting their new password to be the same as a recent past password.
8. samAccountName – The logon name used to support clients and servers, also known as your username.
9. displayName – The display name for an object. This is usually the combination of the users' first name, middle initial and last name.

POLICY

1. Password Length must be at least eight (8) characters.
2. Password Complexity - The password contains characters from at least three of the following four categories:
    a. English uppercase characters (A - Z)
    b. English lowercase characters (a - z)
    c. Numbers (0 - 9)
    d. Special Characters (for example: !, $, #, or %)
3. Passwords must meet the following Complexity Requirements as defined by the Active Directory System policy:
    a. Passwords must not contain the user's entire samAccountName (username) value. The samAccountName is checked in its entirety only to determine whether it is part of the password. If the samAccountName is less than three characters long, this check is skipped.

        Example: "emhagen" is the samAccountName for Erin Hagens. When setting a password, Erin will not be allowed to use "emhagen" in the password. Erin could use a portion of the logon name "Hagen..."

    b. Passwords must not contain the user's entire displayName (Full Name) value.
    c. The displayName is validated for delimiters such as; commas, periods, dashes or hyphens, underscores, spaces, pound or hash signs, and tabs. If any of these delimiters are found, the displayName is split and all parsed sections (tokens) are confirmed not to be included in the password. Tokens that are less than three characters in length are ignored, and substrings of the tokens are not checked.

        Example: "Erin M. Hagens" is split into three tokens: "Erin," "M," and "Hagens." Because the second token is only one character long, it is ignored. Therefore, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password.
4. Password Expiration - Ninety (90) days.
5. Account Lockout - After ten (10) incorrect attempts

6. Account Lockout Reset - Thirty (30) minutes
7. Minimum Password Age - One (1) Day
8. Password History - Ten (10) passwords remembered
9. Do not share your password with anyone for any reason; this includes all Geneva students, faculty or staff as well as non-Geneva personnel. In situations where someone requires access to another individual's protected resources, delegation of permission options should be explored with help from Information Technology Services. For example, Microsoft Exchange calendar will allow a user to delegate control of his or her calendar to another user without sharing any passwords. This type of solution is encouraged. Passwords should not be shared even for the purpose of computer repair. An alternative to doing this is to create a new account with an appropriate level of access for the repair person.
10. It is required that your password is changed 90 days. However, you may choose to vary the frequency of password changes based on the privilege or access level of the account. Accounts of greater privilege or access level should have their password changed more frequently and vice versa. This practice prevents someone, who has obtained your password through some means, from continuing to have access to your account.
11. Consider using a passphrase instead of a password. A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters inserted throughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional benefits such as being longer and easier to remember.

    Example: The passphrase "My passw0rd is $uper str0ng!" is 28 characters long and includes alphabetic, numeric and special characters. It is also relatively easy to remember. It is important to note the placement of numeric and symbolic characters in this example as they prevent multiple words from being found in a standard dictionary. The use of blank spaces also makes a password more difficult to guess.
12. Do not write your password down or store it in an insecure manner. As a general rule, you should avoid writing down your password; however in cases where it is necessary to record your password in order to not forget it, the password should be stored in a secure location and properly destroyed when no longer needed (please reference the *Geneva College Information Technology Services - Data Security Policy*). Using a password manager to store your passwords is not recommended unless the password manager incorporates strong encryption and requires authentication prior to use.

RELATED STANDARDS, POLICIES AND PROCESSES

1. Geneva College Information Technology Services - Data Security Policy
2. Geneva College Information Technology Services - Acceptable Use Policy
3. Geneva College Information Technology Services - User Account Policy

EXCEPTIONS

None

DISCLAIMER

None

Appendix A

Rev	Date	By Whom	What
1.0	9/14/2015	Craig Lahtinen	Initial version