Resolution No. 32 of 2021

Town of Clinton Cyber Security Password Policy

BE IT ENACTED BY, the Town Board of the Town of Clinton as follows:

Overview

This policy is intended to establish the policy for effectively creating, maintaining, and protecting passwords at the Town of Clinton, Dutchess County for Town owned electronic equipment (computers, tablets, laptops, and cell phones) and other appropriate electronic equipment.
The Policy is effective June 9, 2021.

Scope

This policy shall apply to all employees, vendors, contractors, and affiliates of Town of Clinton using Town owned electronic equipment, and shall govern acceptable password use on all systems that connect to Town of Clinton network or access or store Town of Clinton data. These passwords are for the login to the Town's electronic equipment and not for the application programs signing in.

Policy

Password Creation

1. All user and admin passwords must be at least 10 characters in length. Longer passwords and passphrases are strongly encouraged.
2. Passwords must be completely unique and not used for any other system, application, or personal account.

Password Aging

1. User passwords will automatically need to be changed every 30 days by the system. You must change the actual password. Previously used passwords may not be reused for 1 year.
2. System-level passwords must be changed on a monthly basis also and your IT Vendor will handle these password changes. They will also be enforced in the same way as end user passwords using the same rules.
3. If there is a problem with your password, contact the IT Vendor for help.

Password Complexity

Password complexity must meet Microsoft Active Directory password complexity requirements.

1. Must Be at least 10 characters long
2. Must contain a combination of the following:
    1. Upper Case letters
    2. Lower Case letters
    3. Numbers
    4. Special Characters

These complexity requirements will be dictated by and enforced by the Microsoft Active Directory system. If when you are changing your password, you do not follow the above complexity requirements, the system will not let you change your password and you will remain unable to login to your electronic equipment.

Password Protection

1. Passwords must not be shared with anyone (including coworkers and supervisors), and must not be revealed or sent electronically.
2. Passwords shall not be stored on electronic equipment.
3. When configuring password "hints," do not hint at the format of your password (e.g., "zip + middle name")
4. User IDs and passwords must not be stored in an unencrypted format.
5. User IDs and passwords must not be scripted to enable automatic login.
6. "Remember Password" feature on websites and applications should not be used.
7. All Town owned mobile devices (tablets, laptops, and cell phones) that connect to the Town's network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

Enforcement

It is the responsibility of the end user to comply with the policies above and further to remember their passwords and usernames.

With respect to the timing and complexity of password changes, the Active Directory system on the server ensures compliance by not allowing insecure passwords and not allowing passwords to be valid for more than 30 days. Additionally, the system disallows the re-use of passwords for 1 year once they have been used.

If you believe your password may have been compromised, please immediately report the incident to the Town Supervisor, the Town Clerk, and our IT Support vendor and change the password or request an immediate password change from IT Support.

June 8, 2021

Carol-Jean Mackin, Town Clerk