Town of Leyden Password Policy

Date adopted by Select Board: January 30, 2023

Municipalities have an obligation to protect confidential information. Moreover, municipal systems are frequent targets for expensive and embarrassing cyberattacks. While password protection does not in itself safeguard Town systems and data, it is a critical first-line defense for access control.

Policy application.

This policy applies to all Town employees, elected and appointed officials, and volunteers who have or are responsible for an account (or any form of access that supports or requires a password) on a system that resides in any Town facility, has access to a Town network, or stores any non-public Town information (excluding Police Department network and systems).

Password construction.

DO:

- Passwords shall be a minimum of 8 characters in length, though ideally 12 characters or more.
- Passwords shall include at least one of each of the following:
    - Upper case letters
    - Lower case letters
    - Numbers
    - Symbols such as punctuation or special characters
- There are many strategies to help construct strong and easy-to-remember passwords, even if you have many different passwords; see resources below for help.

DON'T DO:

- Passwords shall not include obvious sequences of letters or numbers of three or more characters, such as 123 or abc or qwerty.
- Passwords shall not use words without modification that can be found in the dictionary or might be guessable because they include personal information such family members or pet names, birthdates, addresses, phone numbers, locations, and the like.

Password change and reuse.

- Password shall not be reused on multiple accounts or systems. Each account should have its own password.
- Passwords shall be changed at least every twelve months. Old passwords shall not be reused. The municipal assistant will send out reminders to change passwords, but the Town of Leyden has no systems in place to monitor password change, so it is the responsibility of each individual to whom this policy applies to comply with this requirement.

Password confidentiality.

- Users shall not disclose their passwords to anyone;
- Users shall not share their passwords with others (co-workers, supervisors, family, etc.) unless co-workers are required to sign in through a single account;
- Users shall not write down their passwords and leave them unsecured;
- Users shall not check the "save password" box when authenticating to applications;
- Users shall not use the same password for different systems and/or accounts;
- Users shall not send passwords via email;
- Users shall not reuse passwords.

Incident reporting.

- Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the municipal assistant.
- Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported.
- When a password is suspected to have been compromised the Town will request that the user, or users, change all their passwords.

Highly sensitive data.

For systems and data that are particularly sensitive, including those for which a breach could have serious financial, privacy, or legal consequences, consider more advanced authentication methods. Two-stage authentication, for example, confirms a login with a text message or phone call. Some systems require a physical token/key in combination with a password. The municipal assistant can help you with this or put you in touch with our IT consultant.

Resources.

- https://www.mass.gov/guides/password-best-practices-and-recommendations
- See the municipal assistant if you have questions or need help.