City of Port Townsend Information Technology Policy
Password Policy

Policy

General requirements:

- Except for coordinating password creation and changes with the IT department, passwords will NEVER be shared with anyone.[1]
- Passwords must not be sent through email.
- Passwords must not be reused. Personal passwords should not be used as City passwords and vice versa.
- If an employee suspects that their password has been compromised, that user will contact Information Technology for assistance and recommendations on mitigating risk to the City.
- Passwords must not be stored in plain text on any form of media.

Requirements for password categories:

User Accounts:

All user accounts within the City of Port Townsend (hereafter "the City") will adhere to the following standards and best practices regarding passwords:

1. Passwords shall be a minimum of 11 characters and may contain any combination of uppercase, lowercase, number, spaces, or special characters.
2. Password cannot:
   a. repeat any previous 10 passwords.
   b. contain your username.
   c. contain any part of your full name.
   d. contain 3 or more repeating consecutive characters.
   e. contain repeating patterns of 4 or more characters.
   f. be in the list maintained by HaveIBeenPwned.
3. If the password is less than 15 characters, it will be checked against a dictionary of frequently used words and phrases.

User accounts will expire every 90 days from the time that the password was last set.
User accounts are not allowed to be set to never expire.

Service Accounts:

All service accounts[2] within the City of Port Townsend shall meet the following:

1. All requirements of User Accounts.
2. Passwords shall be a minimum of 64 characters or the maximum allowed by the device.
3. Expire every 6 months.

[1] City of Port Townsend Employee Manual – "*Connecting to the City network, or any specific software package, utilizing somebody else's security identification login information to gain alternate security permissions; gaining unauthorized access to another employee's e-mail messages, or sending messages using another employee's password.*"

[2] A service account is a user account that's created explicitly to provide a security context for services that are running on Windows Server operating systems.

Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of data maintained by the City by mitigating risks associated with weak passwords and practices.

Applicability and Audience

This policy applies to all employees and elected officials of the City and to all information technology resources, communications systems, and equipment owned, leased, rented, established, or otherwise administered by the City. Violations of this policy expose the City to significant cyber security risk. Employees who violate this policy may be disciplined up to and including termination.

Definitions

Media – communication outlet or tool used to store and deliver information or data. This includes but is not limited to USB drives, post-it notes, or digital files.

Exceptions

Any exceptions to this policy must be requested in accordance with the City of Port Townsend Information Technology Formal Exception Policy.

Implementation

This policy shall be effective immediately upon adoption and shall supersede all policies previously adopted by the City. The most current version of this policy will be made available in the “Employee Pages” on the City website. Elected or appointed officials and employees are responsible for understanding and agreeing to abide by all provisions of this policy. The City Manager shall have the authority and responsibility for the implementation of this policy and may make interpretations of issues that are not clearly articulated or not included herein.

Supporting CIS controls
4.1 Establish and Maintain a Secure Configuration Process
5.2 Use Unique Passwords