

City of Port Townsend Information Technology Policy Cyber-Security Awareness Training

Policy

Every City Employee and anyone with a City of Port Townsend email address must take the City's designated Cyber Security awareness training and pass the associated test within 3 weeks of being assigned the training. Additionally, every City Employee and anyone with a City of Port Townsend email address must complete and pass any cyber security training assigned due to failing a phishing test within 2 weeks of being assigned the training.

Failure to take these trainings and pass the tests within the allotted time will result in the user's network account being disabled. The account will be re-enabled once the user has passed the test and informed the Finance Director of said completion.

Purpose

The purpose of this policy is to meet the requirements of the City's insurance provider and to promote security awareness among City Staff and to minimize the risk of compromising City data and infrastructure.

Applicability and Audience

This policy applies to all employees and elected officials of the City and to anyone with a City of Port Townsend email address. Violations of this policy expose the City to significant cyber security risk. Employees who violate this policy will have their network accounts disabled. Repeat offenses may result in other discipline up to and including termination.

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. Everyone with a City email address is responsible for understanding and agreeing to abide by all provisions of this policy. The City Network Administrator 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 controls¹

- 14 Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

¹ <https://www.cisecurity.org/controls/v8>