


CITY OF LARGO ADMINISTRATIVE POLICIES AND PROCEDURES MANUAL	
Policy: Cybersecurity Awareness and Training Program	Policy Number: T-20-10
Originating Department/Division: Information Technology (IT)	
Effective Date: May 01, 2020	Approved By: 
Supersedes Policy: N/A	Dated: 05/01/2020

## PURPOSE

Cybersecurity is the top priority for our organization as a whole and is everyone's responsibility. We must work together to keep the City's digital data safe and accurate. This will be accomplished by maintaining a strong Cybersecurity technical framework and working with City leadership to provide education, training, and testing to help staff learn how to spot and defend against those attempting to compromise our data and/or our computer systems.

## DEFINITIONS

**Cybersecurity** is the protection of Internet-connected systems, including hardware, software and data, from Cyber attacks and unauthorized access.

**Awareness** implies a basic level of understanding about a broad range of information security matters. Awareness tends to be delivered by multiple communications methods such as seminars, case studies, written briefings, reference materials, posters and conversations.

**Training** implies more narrowly-focused and detailed attention to one or more specific topics. Training tends to be delivered through classroom or online courses.

## POLICY

Technical controls are a vital part of the City's information security framework and are not in themselves sufficient to secure all the City's digital information assets. Effective Cybersecurity requires the awareness and proactive support of all City staff, supplementing and making full use of the technical security controls. The City's information, data, and computer network is only as strong as each individual's ability to effectively identify and defend against unauthorized attempts to compromise our systems.

The implementation of a Cybersecurity awareness and training program is intended to give City employees a working understanding of basic Cybersecurity principles and precautions. This training prepares individuals to recognize and prevent falling victim to hacking attempts, Phishing, and Malware infections. It will also assist with recognizing situations and/or behaviors that might compromise both their personal information and/or City data.

This policy applies to all employees who have a City network account, a City email account and/or utilize a City computer to perform their job functions. This policy also applies to third-party employees and vendors working for the organization to comply with our information security policies.

All new qualifying employees must complete their initial Cybersecurity awareness training within two weeks of the time of their account creation as part of their required on-boarding. Employees with access to sensitive data and/or critical systems may be required to complete additional Cybersecurity awareness training commensurate with their job responsibilities. Participation in Cybersecurity awareness training is required for users in order to maintain access to the City network and City email.

Department Directors are responsible for ensuring department staff and other workers within their remit complete the required Cybersecurity awareness training and educational activities within the prescribed time frame. Directors will be provided periodic snapshot reports on their staff's training completion status.

A minimum of one Cybersecurity awareness training course will be offered each year in October, to

coincide with National Cybersecurity Awareness Month and employees will be given a three (3) week time frame in which to complete the training.

If the individual does not complete the Cybersecurity awareness training within the prescribed time frame, the employee, their supervisor and their director will be contacted indicating that the employee has not satisfactorily completed the training. Repeated failure to comply will result in disciplinary action consistent with the City's Code of Conduct.

Employees will receive random Cybersecurity awareness exercises to help solidify the concepts learned in the Cybersecurity awareness training program. The analysis of the exercises will determine the effectiveness of the Cybersecurity awareness training. Should an employee fall victim to one or more of these exercises (Phishing campaign) within a 6 month period, the following corrective actions will apply:

Number of Times Falling Victim	1	2	3
Employee Redirected to Web page Revealing the Phish Results	X	X	X
Supervisor & Director Notification & Employee Coaching	X	X	X
Additional Online Security Awareness Training	X	X	
Department On-Site Training in Coordination with IT Department		X	
Code of Conduct Initiated (Safety Violation)			X

At the end of each Phishing campaign, a success report will be provided to Department Directors.

Resources for learning more about Cybersecurity can be found at [TeamLargo.com/security](http://TeamLargo.com/security).