COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	CYBERSECURITY AWARENESS TRAINING POLICY	ITEM NUMBER:	ITAM-0510
OWNER:	DEPARTMENT OF GENERAL SERVICES	ADOPTION DATE:	MM/DD/2019
APPROVER(S):	COUNTY BOARD OF SUPERVISORS	REVIEW DATE:	MM/DD/2022
VERSION:	1.2	PAGE:	PAGE **1** OF **3**

I. Purpose

This policy establishes the requirement that individuals who access County networks or systems must successfully complete annual cybersecurity awareness training.

II. Audience

The audience for this policy is all County employees, contractors and third parties who access County networks or systems.

III. Scope

This policy applies to anyone doing business as the County and/or in support of the County that is provisioned access to County networks or systems. This includes employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties.

IV. Definitions

1. Breach of Contract: A breach of contract occurs when a party to a contract fails to fulfill his or her obligation as described in the contract.

2. Chief Information Security Officer (CISO): The CISO is a senior-level individual responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

3. Cybersecurity Awareness Training: A formal process for educating employees about computer security.

4. Information Technology (IT): the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.

5. Security Breach: Any incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms.

V. Policy

County of Santa Barbara employees are fully trained to understand the risks of using information technology, how to defend against malicious threats, and how to react to information security events or incidents, whether at a County building or from a remote location. This training is also mandatory to all contractors and third parties who routinely access County IT assets. Without such training, information systems employees have an increased likelihood of breaching security and have lower individual culpability should they breach security.

- Newly hired employees and contractors are required to complete training as soon as administratively possible, not to exceed 30 days.

- Training will be administered through an online program managed by the Department of General Services (GS), Information & Communications Technology (ICT) division.

- The County CISO will be responsible for leading the overall cybersecurity training and awareness program to include not only annual training but any additional training for specific roles or areas.

1. Applicable Rules, Laws, and Regulations:

    i. FBI Criminal Justice Information Services Security Policy

    ii. Health Insurance Portability and Accountability Act of 1996

    iii. IRS Publication 1075

    iv. Payment Card Industry Data Security Standard

2. Exceptions:

    i. Employees who are not provisioned account access to County networks are not required to complete training. County departments that conduct their own cybersecurity awareness training may not be required to complete training offered by ICT provided the training fulfills the following basic security elements that address: social engineering, email security, web browsing, remote access, privacy and data security.

    ii. Contractors and third parties who are not provisioned account access to County networks are not required to complete training. Contractors and third party users holding County-issued accounts are required to sign an agreement, prior to account issuance, which stipulates the completion of annual cybersecurity awareness training within their respective organization. This training must include security elements that address: social engineering, email security, web browsing, remote access, privacy and data security.

3. Non-Compliance: County department heads will be held accountable for their department's completion of the cybersecurity training as a requirement in their annual Employee Performance Review (EPR). Contractors and third parties may face contractual penalties for breach of contract.

4. Related Policies: N/A

5. Referenced Documents: N/A

6. Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	Thomas Gresham	06/18/2018
1.1	Policy Committee Draft Revision	Thomas Gresham	08/13/2018
1.2	EITC requested modifications	Thomas Gresham	02/01/2018