Attachment 5

Security Awareness and Training Policy - ITAM-0611

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

Subject:	County Security Awareness and Training Policy	Item Number:	ITAM-0611
Owner:	Department of General Services	Adoption Date:	MM/DD/20YY
Approver(s):	County Board of Supervisors	Review Date:	MM/DD/20YY
Version:	1.0	Page:	Page **1** of **4**

I. Purpose

To ensure that the appropriate level of information security awareness training is provided to all users of County Information Technology (IT).

II. Audience

The primary audience for this policy is Information Technology Professionals (County executives, managers, employees, contractors, vendors, and third parties) whose responsibilities include managing, administering, and operating County networks or systems.

III. Scope

This policy applies to any Information System that electronically generates, receives, stores, processes or transmits County-owned data, whether the system is hosted on the County network or by a third-party provider. Additionally, these provisions apply 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, collectively referred to hereafter as “agents”.

IV. Definitions

See ITAM-0602, Glossary of Definitions

V. Policy

It is the policy of the County Board of Supervisors that:

Central IT and Departments must ensure all information system users and managers are knowledgeable of security awareness material before authorizing access to systems. Central IT and Departments must identify personnel with information system security roles and responsibilities, document those roles and responsibilities, and provide sufficient security training before authorizing access to information systems or confidential information. Central IT and Departments must document and monitor individual information system security training activities including basic security awareness training and specific information system security training. The following outlines the minimum security control requirements which all information systems must adhere to in order to operate in a production environment.

1. SECURITY AWARENESS TRAINING

a. Schedule security awareness training as part of initial training for new users by use of face to face, document, video, or other appropriate awareness training.

b. Schedule security awareness training when required by information system changes and then annually thereafter.

c. County or Departmental IT shall determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:

i. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.

ii. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

iii. Provide training to specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.

2. SECURITY AWARENESS / INSIDER THREAT

a. Include security awareness training on recognizing and reporting potential indicators of insider threat.

3. ROLE-BASED SECURITY TRAINING

a. Provide role-based security training to personnel with assigned security roles and responsibilities:

i. Before authorizing access to the information system or performing assigned duties.

ii. When required by information system changes and annually thereafter.

b. Designate County personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

4. PHYSICAL SECURITY CONTROLS

   a. Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).

   b. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

5. PRACTICAL EXERCISES

   a. Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

6. SECURITY TRAINING RECORDS

   The County shall:

   a. Designate County personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

   b. Retain individual training records for a minimum of three years.

VI. Exceptions

See ITAM-0600, IT Security Program

VII. Non-Compliance

See ITAM-0600, IT Security Program

VIII. References and Sources

1. Applicable Rules, Laws, and Regulations:

   a. National Institute of Standards and Technology (NIST) Special Publications:

NIST SP 800-53 – Awareness and Training (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100.

b. Electronic Code of Federal Regulations (CFR): 5 CFR 930.301.

c. State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

2. Related Policies:

3. Referenced Documents:

4. Revision History:

VERSION	CHANGE	AUTHOR	DATE OF CHANGE
1.0	Initial Release	CISO/Policy Committee	08/25/2021