Attachment 15

Planning Policy - ITAM-0621

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	PLANNING POLICY	ITEM NUMBER:	ITAM-0621
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 **5**

I. Purpose

To ensure that County Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

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:

Security planning controls include system security plans and system security plan (SSP) updates. Agencies must develop, document, and establish a system security plan by describing the implementation needed to meet security requirements, current controls, and planned controls for protecting information systems and confidential information. The system security plan must be updated on a regular basis to account for significant changes in the security requirements, current controls, and planned controls for protecting information systems and confidential information.

IT security planning is an important quality control tool that helps improve the protection level of IT assets. All systems have some level of sensitivity and require protection as part of good management practices. The IT security planning process encompasses the following components:

- Documentation of security and privacy controls in an SSP

- System Authorization
- Security training, awareness, and education

System owners are accepting the associated risk of information loss, system misuse, unauthorized system access or modification, system unavailability, and undetected system activities. Good security planning, therefore, serves an important risk management function by providing the necessary information to determine the type and level of risks, and to base decisions on risk acceptance or mitigation. Managers must also be assured that all personnel accessing the system, from those performing system management functions to general users, have received security training at levels commensurate with the duties they perform. The following outlines the minimum security control requirements which all information systems must adhere to in order to operate in a production environment.

1. SYSTEM SECURITY PLAN

County IT or Departmental IT shall:

a. Develop a security plan for each information system that:

i. Is consistent with the County's enterprise architecture.

ii. Defines explicitly the authorization boundary for the system.

iii. Describes the operational context of the information system in terms of missions and business processes.

iv. Provides the security categorization of the information system including supporting rationale.

v. Describes the operational environment for the information system and relationships with or connections to other information systems.

vi. Provides an overview of the security requirements for the system.

vii. Identifies any relevant overlays, if applicable.

viii. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions.

ix. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the security plan and communicate subsequent changes to the plan to authorized personnel and/or business units.

c. Review the security plan for the information system at least annually.

d. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

e. Protect the security plan from unauthorized disclosure and modification.

2. RULES OF BEHAVIOR

County IT or Departmental IT shall:

a. Establish, and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage.

b. Receive a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

c. Review and update the rules of behavior.

d. Require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised and updated.

3. INFORMATION SECURITY ARCHITECTURE

County IT or Departmental IT shall:

a. Develop information security architecture for the information system that will:

i. Describe the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information.

ii. Describe how the information security architecture is integrated into and supports the enterprise architecture.

iii. Describe any information security assumptions and dependencies on external services.

b. Review and update the information security architecture no less than annually, to reflect updates in the enterprise architecture.

c. Ensure that planned information security architecture changes are reflected in the security plan, the security operations, and County

procurements/acquisitions.

4. DEFENSE-IN-DEPTH APPROACH

County IT or Departmental IT shall:

a. Design security architecture using a defense-in-depth approach that:

i. Allocates security safeguards to county defined locations and architectural layers.

ii. Will ensure that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.

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 (SP):

iii. NIST SP 800-53a – Security Planning (PL)

iv. NIST SP 800-12

v. SP NIST 800-18

vi. NIST SP 800-100

b. 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:

SUBJECT:	PLANNING POLICY	ITEM NUMBER:	ITAM-0621
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 **5** OF **5**

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