Attachment 7

Security Assessment and Authorization Policy - ITAM-0613

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	SECURITY ASSESSMENT AND AUTHORIZATION POLICY	ITEM NUMBER:	ITAM-0613
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 **6**

I. Purpose

County Information Technology (IT) and the County's various business units (information owners) will ensure security controls in information systems, and the environments in which those systems operate, as part of initial and ongoing security authorizations, annual assessments, continuous monitoring, and system development life cycle activities.

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". This policy is applicable to all County departments and users of County resources and assets. Every County department that maintains or collects informational assets must be compliant with this policy.

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 produce an Authorization to Operate (ATO) document that verifies security controls have been adequately implemented (or plan to be implemented) to protect confidential information. The ATO constitutes the agency's acknowledgment and acceptance of risk associated with the system. Custodians of confidential information will verify the completeness and propriety of the security controls used to protect confidential information before initiating operations. This must be done for any infrastructure component or system associated with confidential information. This process must occur every three (3) years or whenever there is a significant change (e.g., major software upgrade, implementation of new hardware, change of hosting services, etc.) to the control structure. A senior Central IT or Department official must sign and approve the security authorization.

Central IT or Departments must continuously (at least annually) monitor the security controls within their information systems to ensure that the controls are operating as intended. Central IT or Department s must authorize and document all connections from information systems to other information systems outside of the system boundary using service interface agreements and monitor/control system connections on an ongoing basis.

Central IT or Departments must annually conduct a formal assessment of the security controls of information systems to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting applicable security requirements. Agencies are responsible for identify any deficiencies related to the processing of confidential information and implementation of requirements. The analysis must identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during annual assessments. A Corrective Action Plan (CAP) will identify activities planned or completed to correct deficiencies identified during the Security Assessment review. Both the analysis and the CAP must address implementation of security controls to reduce or eliminate known vulnerabilities in agency systems. 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 ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

The County shall:

a. Develop, document, and disseminate to appropriate technology and supporting staff:

i. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

ii. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.

b. Review and update the current security assessment and authorization policy and procedures annually.

2. SECURITY ASSESSMENTS

The County shall:

a. Develop a security assessment plan that describes the scope of the assessment including:

i. Security controls and control enhancements under assessment.

ii. Assessment procedures to be used to determine security control effectiveness.

iii. Assessment environment, assessment team, and assessment roles and responsibilities.

b. Assess the security controls in the information system and its environment of operation annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

c. Produce a security assessment report that documents the results of the assessment.

d. Provide the results of the security control assessment to the County CIO.

3. SYSTEM INTERCONNECTIONS

County IT or Departmental IT shall:

a. Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements.

b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.

c. Review and update appropriate Interconnection Security Agreements annually.

d. Employ permit-by-exception policy for allowing internal staff to connect to external information systems.

e. Authorize internal connections of defined and appropriate technology assets and systems by direction of the County CIO.

f. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

4. PLAN OF ACTION AND MILESTONES

The County shall:

a. Develop a plan of action and milestones for the information system to document the County's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

b. Update existing plan of action and milestones annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

5. SECURITY AUTHORIZATION

The County shall:

a. Assign a senior-level executive or manager as the authorizing official for the information system. For those departments with IT support staff, the County's CISO will provide assistance.

b. Ensure that the authorizing official authorizes the information system for processing before commencing operations.

c. Update the security authorization at least annually or as needed during modification to existing systems and deployment of new systems.

6. CONTINUOUS MONITORING

County IT or Departmental IT shall:

a. Develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

i. Establishment of best industry practices and recommendations systems as defined by IT to be monitored.

ii. Establishment of best industry practices and recommendations frequencies for monitoring and within IT defined frequencies for assessments supporting such monitoring.

iii. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy.

iv. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy.

v. Correlation and analysis of security-related information generated by assessments and monitoring.

vi. Response actions to address results of the analysis of security-related information.

vii. Reporting the security status of organization and the information system to County CIO annually.

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):

i. NIST SP 800-53a – Security Assessment and Authorization (CA)

ii. NIST SP 800-12

iii. NIST SP 800-37

iv. NIST SP 800-39

v. NIST SP 800-47

vi. NIST SP 800-100

vii. NIST SP 800-115

viii. NIST SP 800-137

b. NIST Federal Information Processing Standards (FIPS) 199

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