Attachment 16

Personnel Security Policy - ITAM-0623

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	PERSONNEL SECURITY POLICY	ITEM NUMBER:	ITAM-0623
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

To ensure that personnel security safeguards are applied to the access and use of information technology resources and data

II. Audience

The primary audience for this policy is Information Technology Professionals (County executives, managers, employees, contractors, vendors, and third parties) whose responsibilities including 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:

Physical access to information technology processing equipment, media storage areas, and media storage devices and supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas.

Central IT and Departments are responsible for:

- Ensuring proper employee/contractor identification processes are in place;
- Conducting background investigations during the hiring process
- Ensuring that employees/contractors receive annual training in regards to physical security best practices.

The following outlines the minimum security control requirements which all County information systems must adhere to in order to operate in a production environment.:

1. POSITION RISK DESIGNATION

County Information Technology (IT) shall:

a. Assign a risk designation to all County positions based on County IT or Departmental IT established categories.

b. Establish screening criteria for individuals filling those positions.

c. Review and update position risk designations annually.

2. PERSONNEL SCREENING

County IT or Departmental IT and department system and application owners shall:

a. Screen individuals prior to authorizing access to the information systems.

b. Rescreen individuals according to appropriate security processes that have been pre-determined.

c. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

3. PERSONNEL TERMINATION

County IT or Departmental IT and departments shall, upon termination of individual employment:

a. Disable information system access within the shortest period of time, preferably just prior to termination.

b. Terminate/revoke any authenticators/credentials associated with the individual.

c. Conduct exit interviews that include a discussion of having any protected and confidential data or information or having access to such systems. This includes physical copies of such data and information.

d. Retrieve all security-related County information system-related property.

e. Retain access to County information and information systems formerly controlled by terminated individual.

f. Notify County IT or Departmental IT Staff immediately as soon as termination is determined.

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.

The County shall:

g. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of county information.

h. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the county termination process as directed by County Counsel and Human Resources (HR).

i. Employ automated mechanisms to notify IT, General Services, and those departments responsible for physical access upon termination of an individual to disable access to technology assets or physical access.

4. PERSONNEL TRANSFER

County IT and departments shall:

a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the County.

b. Initiate the County employee departmental transfer process to insure rights and access to protected and confidential data and information based of rules and regulations continue to be protected.

c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

d. Notify County IT immediately or as soon as possible of transfer.

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

5. ACCESS AGREEMENTS

County IT and departments shall:

a. Develop and document access agreements for County information systems.

b. Review and update the access agreements at least annually.

c. Ensure that individuals requiring access to County information and information systems:

   i. Sign appropriate access agreements prior to being granted access.

   ii. Re-sign access agreements to maintain access to County information systems when access agreements have been updated or on an annual basis.

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

6. THIRD-PARTY PERSONNEL SECURITY

County IT or Departmental IT shall:

a. Establish and document personnel security requirements including security roles and responsibilities for third-party providers.

b. Require third-party providers to comply with personnel security policies and procedures established by the County.

c. Require third-party providers to notify County IT or Departmental IT of any personnel transfers or terminations of third-party personnel who possess County credentials and/or badges, or who have information system privileges within 24 hours of said event.

d. Monitor provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

7. PERSONNEL SANCTIONS

County IT and County HR shall:

a. Employ existing HR's recommendations and process for individuals failing to comply with established information security policies and procedures.

b. Notify County Human Resources Department as soon as knowledge of potential sanction when a formal employee sanctions process is initiated, identifying the

individual sanctioned and the reason for the sanction.

County sanction processes reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for those organizations.

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 – Personnel Security (PS)
      ii. NIST SP 800-12
      iii. NIST SP 800-60
      iv. NIST SP 800-73
      v. NIST SP 800-78
      vi. NIST SP 800-100
   b. Electronic Code of Federal Regulations (CFR): 5 CFR 731.106.
   c. Federal Information Processing Standards (FIPS)
      i. 199
      ii. 201
   d. Intelligence Community Directive (ICD) 704 Personnel Security Standards.
   e. State of California State Administrative Manual (SAM) 5300 et seq.

i. 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