Attachment 8

County Configuration Management Policy - ITAM-0614

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	CONFIGURATION MANAGEMENT POLICY	ITEM NUMBER:	ITAM-0614
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 **7**

I. Purpose

To ensure that County Information Technology (IT) resources are inventoried and configured in compliance with County IT security policies, standards, and procedures, along with applicable State and Federal requirements.

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:

System hardening procedures must be created and maintained to ensure up-to-date security best practices are deployed at all levels of the IT systems (operating systems, applications, databases and network devices). All default system administrator passwords must be changed. Central IT and Departments must implement an appropriate change management process to ensure changes to the systems are controlled by:

- Developing, documenting, and maintaining current secured baseline configurations.
- Network devices should be patched and updated for all security related updates/patches using automated tools when possible.
- Develop, document, and maintain a current inventory of the components of information systems and relevant ownership information.
- Configuring information systems to provide only essential capabilities.
- Configuring the security settings of information technology products to the most restrictive mode consistent with operational requirements.

- Analyzing potential security impacts of changes prior to implementation.
- Authorizing, documenting, and controlling system level changes.
- Restricting access to system configuration settings and provide the least functionality necessary.
- Prohibiting the use of functions, ports, protocols, and services not required to perform essential capabilities for receiving, processing, storing, or transmitting confidential information.

Maintaining backup copies of hardened system configurations. Configuration management describes the processes through which baseline configurations are developed and maintained for information systems and their constituent components. System configurations must be compliant with security requirements, and all changes to system configurations must be controlled and approved. The process of configuration management provides for a controlled environment in which changes to software and hardware are properly authorized, tested, and approved before implementation. 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. BASELINE CONFIGURATION

County ICT or Departmental IT shall:

a. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.

b. Review and update the baseline configuration of the information system annually.

c. Review and update the baseline configuration of the information system when required as a result of changes to the system including deployment of new system components and as an integral part of information system component installations and upgrades.

d. Retain one previous version of baseline configurations of information systems to support rollback.

2. CONFIGURATION CHANGE CONTROL

County IT or Departmental IT shall:

a. Determine the types of changes to the information system that are configuration-controlled.

b. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses with an established by County IT or Departmental IT process.

c. Document configuration change decisions associated with the information system.

d. Implement approved configuration-controlled changes to the information system.

e. Retain records of configuration-controlled changes to the information system for a minimum of three years.

f. Audit and review activities associated with configuration-controlled changes to the information system.

g. Coordinate and provide oversight for configuration change control activities through appropriate change control processes that convenes as needed and as defined by the County CIO.

h. Test, validate, and document changes to the information system before implementing the changes on the operational system.

3. SECURITY IMPACT ANALYSIS

County IT or Departmental IT shall:

a. Analyze changes to the information system to determine potential security impacts prior to change implementation.

4. ACCESS RESTRICTIONS FOR CHANGE

County IT or Departmental IT shall:

a. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

5. CONFIGURATION SETTINGS

County IT or Departmental IT shall:

a. Establish and document configuration settings for information technology products employed within the information system using documentation contained within appropriate IT systems folders that reflect the most restrictive mode consistent with operational requirements.

b. Implement the configuration settings.

c. Identify, document, and approve any deviations from established configuration settings for all critical technology assets based on County IT or Departmental IT defined operational requirements.

d. Monitor and control changes to the configuration settings in accordance with County policies and procedures.

6. LEAST FUNCTIONALITY

County IT or Departmental IT shall:

a. Configure the information system to provide only essential capabilities.

b. Review the information system at least annually or more frequently as need dictates to identify unnecessary and/or non-secure functions, ports, protocols, and services.

c. Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.

d. Prevent program execution in accordance with County policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.

e. Identify software programs not authorized to execute on information systems.

f. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

g. Review and update the list of unauthorized software programs annually.

7. INFORMATION SYSTEM COMPONENT INVENTORY

County IT or Departmental IT shall:

a. Develop and document an inventory of information system components that:

i. Reflects the current information system accurately.

ii. Includes all components within the authorization boundary of the information system.

iii. Is at the level of granularity deemed necessary for tracking and reporting.

iv. Includes information deemed necessary to achieve effective information system component accountability.

b. Review and update the information system component inventory no less than annually.

c. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.

d. Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the information system.

e. Take the following actions when unauthorized components are detected:

i. Disable network access by such components, or

ii. Isolate the components and notify the Chief Information Officer and system owner.

f. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

8. CONFIGURATION MANAGEMENT PLAN

County IT or Departmental IT shall develop, document, and implement a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures.

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.

c. Defines the configuration items for the information system and places the configuration items under configuration management.

d. Protects the configuration management plan from unauthorized disclosure and modification.

9. SOFTWARE USAGE RESTRICTIONS

County IT or Departmental IT shall:

a. Use software and associated documentation in accordance with contract agreements and copyright laws.

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

10. USER-INSTALLED SOFTWARE

County IT or Departmental IT shall:

a. Establish policies governing the installation of software by users.

b. Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.

c. Monitor policy compliance at least 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 Publication (SP):

i. NIST SP 800-53a – Configuration Management (CM)

b. State of California State Administrative Manual (SAM) 5300 et seq.

c. 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