Attachment 19

# System and Communications Protection Policy - ITAM-0627

# COUNTY OF SANTA BARBARA
# INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

| | | | |
|---|---|---|---|
| SUBJECT: | SYSTEM AND COMMUNICATIONS PROTECTION POLICY | ITEM NUMBER: | ITAM-0627 |
| 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 **8** |

## I. Purpose

To establish guidelines for system and communications protection for County Information Technology (IT) resources and information systems.

## 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:

The System and Communications Protection control family describes the technical mechanisms that an organization can employ to provide a baseline defense against basic system and communication attack methods. Most of the control mechanisms are designed to be implemented at the server and network tier of the enterprise computing environment; however, selected controls may apply to enterprise applications as well. Common themes, including segmenting computing resources and applying data encryption characterize the system and communications protection control family. 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. APPLICATION PARTITIONING

County IT or Departmental IT shall:

a. At every opportunity and within existing resources, separate user functionality from information system management functionality either logically or physically.

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.

2. INFORMATION IN SHARED RESOURCES

County IT or Departmental IT shall:

a. Prevent unauthorized and unintended information transfer via shared system resources.

This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

3. DENIAL OF SERVICE PROTECTION

County IT or Departmental IT shall:

a. Ensure that the information system protects against or limits the effects of the following types of denial of service attacks: brute force attack, web defacement, and other public-facing services that are interrupted by employing periodic and frequent review of public-facing services, including web pages, GIS systems, etc.

b. The information system restricts the ability of individuals to launch or limit such denial of service attacks against other information systems.

4. BOUNDARY PROTECTION

County IT or Departmental IT shall:

a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.

b. Implement sub-networks for publicly accessible system components that are [physically; logically] separated from internal organizational networks, and connected to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within security architecture.

5. TRANSMISSION CONFIDENTIALITY AND INTEGRITY

County IT or Departmental IT shall:

a. Deploy information systems that protect the confidentiality and integrity of transmitted information.

This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

6. NETWORK DISCONNECT

County IT or Departmental IT shall:

a. Ensure information systems are configured to terminate the network connection associated with a communications session at the end of the session or after 20 minutes of inactivity; this control applies to both internal and external networks.

Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

7. CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

County IT or Departmental IT shall:

a. Establish and manage cryptographic keys for required cryptography employed within the information system in accordance with existing State and Federal rules and regulations.

8. CRYPTOGRAPHIC PROTECTION

County IT or Departmental IT shall:

a. Implement appropriate cryptographic deployment in accordance with applicable federal and state laws, directives, policies, regulations, and standards.

Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision

of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals.

9. COLLABORATIVE COMPUTING DEVICES

County IT or Departmental IT shall:

a. Prohibit remote activation of collaborative computing devices with the following exceptions: Allowed based on business need and approval of departmental management and IT CIO based on review of security issues of said devices.

b. Provide an explicit indication of use to users physically present at the devices.

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

10. PUBLIC KEY INFRASTRUCTURE CERTIFICATES

County IT or Departmental IT shall:

a. Issue public key certificates under a defined certificate policy or obtain public key certificates from an approved service provider.

b. Manage information system trust stores for all key certificates to ensure only approved trust anchors are in the trust stores.

11. MOBILE CODE

County IT or Departmental IT shall:

a. Define acceptable and unacceptable mobile code and mobile code technologies.

b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

c. Authorize, monitor, and control the use of mobile code within the information system.

Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously.

12. VOICE OVER INTERNET PROTOCOL

County IT or Departmental IT shall:

a. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously. VoIP Systems will use the same security policies, protections, and protection schemas that are applied to every technology asset at the County.

b. Authorize, monitor, and control the use of VoIP within the information system.

13. SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

County IT or Departmental IT shall:

a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service.

14. SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

County IT or Departmental IT shall:

a. Ensure information systems that requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching domain name system (DNS) servers.

15. ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

    County IT or Departmental IT shall:

    a. Ensure the information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

    b. Employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server, to eliminate single points of failure and to enhance redundancy.

Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers.

16. SESSION AUTHENTICITY

    County IT or Departmental IT shall:

    a. Ensure the information system protects the authenticity of communications sessions.

This control addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

17. PROTECTION OF INFORMATION AT REST

    County IT or Departmental IT shall:

    a. Ensure the information system protects the [confidentiality; integrity] of all County of Santa Barbara data, information, and technology assets.

This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems.

18. PROCESS ISOLATION

    County IT or Departmental IT shall:

    a. Ensure, if possible with available resources, the information system maintains a separate execution domain for each executing process.

Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

## 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 SP800-53a - System and Communications Protection (SC)
      ii. NIST SP 800-12
      iii. NIST SP 800-28
      iv. NIST SP 800-41
      v. NIST SP 800-52
      vi. NIST SP 800-56
      vii. NIST SP 800-57
      viii. NIST SP 800-58
      ix. NIST SP 800-77
      x. NIST SP 800-81
      xi. NIST SP 800-95
      xii. NIST SP 800-100

xiii. NIST SP 800-111

xiv. NIST SP 800-113

b. NIST Federal Information Processing Standards (FIPS)

i. (FIPS) 140-2

ii. FIPS 197

iii. FIPS 199

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

d. 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 |
| | | | |