Attachment 14

Physical and Environmental Protection Policy - ITAM-0620

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY	ITEM NUMBER:	ITAM-0620
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 protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

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:

Physical security refers to the provisions of a safe and secure environment for information processing activities. 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.

Physical access controls must be in place for the following:

- Data Centers
- Areas containing servers and associated media
- Networking cabinets and wiring closets
- Power and emergency backup equipment
- Operations and control areas

Each department is responsible for:

- Ensuring proper employee/contractor identification processes are in place.
- Conducting background investigations during the hiring process.
- Ensuring proper environmental and physical controls are established to prevent accidental or unintentional loss of information residing on IT systems.
- Ensuring that any physical access controls are auditable.
- Ensuring that employees/contractors receive annual training in regards to physical security best practices.

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

1. PHYSICAL ACCESS AUTHORIZATIONS

   County IT or Departmental IT shall:

   a. Develop, approve, and maintain a list of individuals with authorized access to the facilities where the information systems reside.

   b. Issue authorization credentials for facility access.

   c. Review the access list detailing authorized facility access by individuals and remove individuals from the facility access list when access is no longer required.

2. PHYSICAL ACCESS CONTROL

   County IT or Departmental IT shall:

   a. Enforce physical access authorizations by verifying individual access authorizations before granting access to the facility.

   b. Control ingress/egress to the facility using appropriate security tools such as locks, access fobs, cameras, alarms or a combination of such safeguards.

   c. Maintain physical access audit logs for sensitive areas containing technology assets or systems containing protected or confidential data or information.

   d. Provide appropriate security safeguards to control access to areas within the facility officially designated as publicly accessible.

e. Escort visitors and monitor visitor activity in sensitive areas.

f. Secure keys, combinations, and other physical access devices.

g. Inventory physical access devices annually.

h. Change combinations and keys no less than annually and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

3. FACILITY PENETRATION TESTING

County IT or Departmental IT shall:

a. Employ a penetration testing process that includes annual, unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

4. ACCESS CONTROL FOR TRANSMISSION MEDIUM

County IT or Departmental IT shall:

a. Control physical access to all County transmission assets and processes within County facilities using industry accepted standards.

5. ACCESS CONTROL FOR OUTPUT DEVICES

County IT or Departmental IT shall:

a. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output of critical operational areas that include PHI, PII, Law and other protected and confidential data.

b. Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by County personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

6. MONITORING PHYSICAL ACCESS

County IT or Departmental IT shall:

a. Monitor physical access to the facility where the information system resides to

detect and respond to physical security incidents.

b. Review physical access logs (if available) minimally monthly and upon occurrence of a suspected event and coordinate results of reviews and investigations with the organizational incident response capability.

7. VISITOR ACCESS RECORDS

County IT or Departmental IT shall:

a. Maintain visitor access records to the facility where the information system resides annually and review visitor access records monthly.

8. POWER EQUIPMENT AND CABLING

County IT or Departmental IT shall:

a. Protect power equipment and power cabling for the information system from damage and destruction.

b. Determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

9. EMERGENCY SHUTOFF

County IT or Departmental IT shall:

a. Provide the capability of shutting off power to the information system or individual system components in emergency situations.

b. Place emergency shutoff switches or devices in critical technology areas to facilitate safe and easy access for personnel; and protect emergency power shutoff capability from unauthorized activation.

10. EMERGENCY POWER

County IT or Departmental IT shall:

a. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system; transition of the information system to long-term alternate power in the event of a primary power source loss.

b. Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

11. EMERGENCY LIGHTING

County IT or Departmental IT shall:

a. Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

b. Provide emergency lighting for all areas within the facility supporting essential missions and business functions.

12. FIRE PROTECTION

County IT or Departmental IT shall:

a. Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

13. TEMPERATURE AND HUMIDITY CONTROLS

County IT or Departmental IT shall:

a. Maintain temperature and humidity levels within the facility where the information system resides at pre-defined levels.

b. Monitor temperature and humidity levels in real time notification processes to include alarms or notifications of changes potentially harmful to personnel or equipment.

14. WATER DAMAGE PROTECTION

County IT or Departmental IT shall:

a. Protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working

properly, and known to key personnel.

This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

15. DELIVERY AND REMOVAL

County IT or Departmental IT shall:

a. Authorize, monitor, and control entering and exiting the facility and maintain records of those items delivered and removed from facility.

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

16. ALTERNATE WORK SITE

County IT or Departmental IT shall:

a. Employ all existing internally deployed security at alternate work sites.

b. Assess as feasible, the effectiveness of security controls at alternate work sites.

c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

Alternate work sites may include, for example, other government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. County staff may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

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 – Physical and Environmental Protection (PE)
      ii. NIST SP 800-46
      iii. NIST SP 800-73
      iv. SP NIST 800-76
      v. SP NIST 800-78
      vi. SP NIST 800-116

   b. Intelligence Community Directive (ICD): 704 705

   c. Department of Defense (DoD): Instruction 5200.39 Critical Program Information (CPI) Protection.

   d. Federal Identity, Credential, and Access Management (FICAM) publication: Personal Identity Verification (PIV) in Enterprise Access Control System (E-PACS) (2012).

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

   f. 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