Attachment 13

Media Protection Policy - ITAM-0619

COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY ADMINISTRATIVE MANUAL

SUBJECT:	MEDIA PROTECTION POLICY	ITEM NUMBER:	ITAM-0619
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 **4**

I. Purpose

The purpose of this policy is to ensure proper precautions are in place to protect confidential information stored on media and to ensure that County Information Technology (IT) controls access to and disposes of media resources in compliance with County IT security policies, standards, procedures, and regulatory agreements, 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:

Central IT and Departments must restrict access to system media containing confidential information to authorized individuals. Media labeled “Confidential” must be physically controlled and securely stored. Central IT and Departments must protect and control “Confidential” system media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. Central IT and Departments must deploy a tracking method to ensure “Confidential” system media reaches its intended destination.

When no longer required for mission or project completion, media to be used by another person within the agency must be overwritten (clear or purge) with software and protected consistent with the classification of the data. Specific procedures must be documented in the applicable agency IT System Security Plan.

Throughout the lifecycle of IT equipment, there are times when Central IT and Departments will be required to relinquish custody of the asset. The transfer of custody may be temporary, such as when the equipment is serviced or loaned, or the transfer may be permanent; examples being a donation, trade-in, lease termination or disposal. Any transfer of custody of equipment poses a significant risk that confidential information, licensed software or intellectual property stored on that equipment may also be transferred. To eliminate the possibility of inadvertently releasing residual representation of state data, state agencies must either destroy the electronic storage media (provide evidence of destruction documentation) or ensure that the electronic storage media has been sanitized in accordance with NIST SP800-88 (R1), Guidelines for Media Sanitization.

Note: Disposal of electronic storage media should be in compliance with Central IT or the Department's respective document retention policy and litigation hold procedures. Several factors should be considered along with the security categorization of the system when making sanitization decisions. Disposal decisions should be made based upon the classification of the data, level of risk, and cost. 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. MEDIA ACCESS:

   County IT through direction from departments shall:

   a. Restrict access to only those staff members assigned to support such media.

   b. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.

2. MEDIA STORAGE

   County IT or Departmental IT shall:

   a. Specify staff to physically control and securely store media within defined controlled areas.

   b. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

3. MEDIA TRANSPORT

   County IT or Departmental IT Shall:

   a. Protect and control media during transport outside of controlled areas.

b. Maintain accountability for information system media during transport outside of controlled areas that may contain protected data and information.

c. Document activities associated with the transport of information system media containing protected data and information.

d. Restrict the activities associated with the transport of information system media to authorized personnel.

4. MEDIA SANITIZATION

County IT or Departmental IT shall:

a. Sanitize prior to disposal, release out of organizational control, or release for reuse using DoD level data wipe processes in accordance with applicable federal and organizational standards and policies.

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

5. MEDIA USE

County IT or Departmental IT shall:

a. Prohibit the use of non-IT approved/supported media on County-owned equipment using unapproved security safeguards.

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 800-53 – Media Protection (MP)

ii. NIST SP 800-12

iii. NIST SP 800-56

iv. NIST SP 800-57

v. NIST SP 800-60

vi. NIST SP 800-88

vii. NIST SP 800-100

viii. NIST SP 800-111

b. NIST Federal Information Processing Standards (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