County Policy Format

County of Santa Clara

Administrative Policies & Procedures Manual

Category: Information Security Sub-category: Storage Media

Policy Name: Removable Storage Media

Policy Number: SCC-RSM

Business Owner Title: Chief Information Security Officer

1.0 Policy Purpose and Summary:

Purpose:

By attaching flash drives, portable hard drives, SD cards, DVDs, CDs, Cameras, and mobile devices Users can easily copy and remove Confidential or Restricted information, as well as inadvertently (*or maliciously*) transfer malware onto County systems.

This policy presents the *minimum* standards related to removable storage media, and if they choose, individual Departments may impose stricter standards within their own environments. For example, Departments may choose to prohibit the use of removable media altogether.

Policy:

22.3.1 Each Department shall have a formal, written policy regarding the use of Removable Storage Media, and shall disseminate this policy to its Users. Departments may use the County-level policy.	Write it down and communicate the policy
22.3.2 The use of Users' personally-owned Removable Storage Media on any County-owned system is prohibited; all Removable Storage Media used with County-owned systems shall be County-owned devices that have been formally issued to the individual User by the User's Department.	Use County approved devices only

22.3.3 Department-issued Removable Storage Media are County property, and shall be used for legitimate County business purposes only. The same rules of conduct and appropriate use standards that apply to County-owned servers, desktop computers and Mobile Devices shall also apply to Removable Storage Media.	Return when finished
22.3.4 Use of Removable Storage Media shall be limited to situations involving the simple transfer of data between computers. Such Media shall not be used as a substitute for performing a formal Backup of data, nor for storing the authoritative and/or only copy of data or files.	Used for data transfer only
22.3.5 Data contained on Removable Storage Media devices shall be protected from alteration or disclosure via both Authentication and privacy measures.	Encrypt the media
22.3.6 Departments shall implement procedures for managing and controlling Removable Storage Media.	Track the media
22.3.7 Departments shall implement methods to prevent the transfer of Malicious Software from Removable Storage Media to County computers.	Scan media for malware
22.3.8 Users issued Removable Storage Media shall be made responsible for the physical security of the device, and every effort shall be made to protect USB Storage Devices from loss or theft.	Don't lose it!
22.3.9 Following loss or theft of a County-owned Removable Storage Media device, the procedures specified in the County's Information Security Incident Response Plan shall be followed.	If you do lose it, contact us immediately
22.3.10All Removable Storage Media shall be treated as any other County-owned computing device for the purpose of device disposal.	Dispose of it per standards

2.0 Related Policies:

Physical Security	-	SCC-PS
Encryption	-	SCC-EN
Data Classification	-	SCC-DC
Mobile Devices	-	SCC-MS

3.0 Standards**, Regulations, Statute Mapping**

ISO27001:2005 standard as mapped to HIPAA, FedRamp, PCI, and NIST 800-53

4.0 Frequently Asked Questions/Scenarios:

Link to overall information security FAQs

5.0 Control Families and Controls (Handbooks):

- SCC-AC
  - AC-3 Access Enforcement
  - AC-16 Security Attributes
- SCC-AU
  - AU-2 Audit Events
  - AU-4 Audit Storage Capacity
  - AU-5 Response to Audit Processing Failures
  - AU-6 Audit Review, Analysis, and Reporting
  - AU-9 Protection of Audit Information
  - AU-12 Audit Generation
- SCC-CM
  - CM-2 Baseline Configuration
  - CM-6 Configuration Settings
- SCC-CP
  - CP-6 Alternate Storage Site
  - CP-9 Information System Backup
- SCC-IA
  - IA-2 Identification and Authentication (*Organizational Users*)
- SCC-MP
  - MP-2 Media Access
  - MP-6 Media Sanitization
  - MP-7 Media Use
- SCC-PE
  - PE-2 Physical Access Authorizations
  - PE-3 Physical Access Control
- SCC-PL
  - PL-2 System Security Plan
  - PL-4 Rules of Behavior
- SCC-RA
  - RA-3 Risk Assessment

County Policy Format

Forms associated with policy:

Countywide policy (*Yes*)

Establishment Date: January 01, 2012

Last Reviewed Date: January 15, 2015

Last Revised Date: January 15, 2015

For internal use Next review date: January 14, 2016

For internal use:

Version Number	Date	Changes made
1	5/8/2013	Removed roles and responsibilities -
2	1/15/2015	Reviewed for publication