# LAC+USC MEDICAL CENTER POLICY

| | | | |
|---|---|---|---|
| | | Page 1 | Of 4 |
| Subject:<br>**DEVICE AND MEDIA CONTROLS** | Original Issue Date: 7/13/10 | Policy # **473** | |
| | Supersedes: 9/22/20 | Effective Date: 10/30/20 | |

| Departments Consulted: | Reviewed & Approved by: | Approved by: |
|---|---|---|
| Information Systems<br>Materials Management | Attending Staff Associations<br>Executive Committee<br>Senior Executive Council | (Signature on File)<br>Chief Medical Officer |
| | | (Signature on File)<br>Chief Executive Officer |

## PURPOSE

The purpose of this policy is to state the requirement for controls that govern the receipt and removal of hardware and/or software (for example, USB flash drives, removable hard drives, and tapes) into and out of LAC+USC Medical Center.

## POLICY

LAC+USC Medical Center shall be responsible for implementing security safeguards that govern the receipt and removal of hardware and electronic media that contain electronic information into and out of LAC+USC Medical Center and the movement of these items within LAC+USC Medical Center.

1. **Disposal**

   Information Technology Management must comply with Device and Media Controls Procedure below to address the final disposition of all information and/or the hardware or electronic media on which it is stored.

2. **Media Re-Use**

   Information Technology Management must remove Protected Health Information (PHI) and other confidential and/or sensitive information before the media are made available for re-use.

3. **Accountability**

   Information Technology Management must be accountable for documenting the movement of hardware and electronic media and any person responsible therefore in a hardware and software inventory system.

4. **Data Backup and Storage**

   Information Technology Management must create a process for storing and retrieving, exact copies of validated electronic information, when needed and before the movement of equipment.

## DEFINITIONS

For a more complete definition of terms used in this policy and/or procedure, see the DHS

Information Security Glossary, Attachment I, **(460-A)** to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

## PROCEDURE

LAC+USC must implement security safeguards that govern the receipt and removal of hardware and electronic media that contain electronic Information into and out of LAC+USC, and the movement of these items within LAC+USC.

### I. Receipt of hardware and software into a Facility

A. Information Technology Management must maintain a secured record documenting all hardware and software received into LAC+USC.

B. Information Technology Management must document all hardware and software according to access, clearance levels, and/or data set type, as needed.

C. Information Technology Management must scan the components (e.g., software, storage devices) for malicious software.

D. Information Technology Management must create a backup of any software received and securely store the backup until the software is no longer in use.

E. Information Technology Management must provide an accounting of all documentation to LAC+USC's CIO at the time of receipt of the hardware and/or software.

### II. Removal of hardware and software from a Facility

A. LAC+USC Information Technology Management must first give written approval before any hardware or software is removed from a Facility.

B. LAC+USC Information Technology Management must consider the reasons for the requested removal of any hardware and software and must consider the requestor's:

1. Access and clearance levels;
2. Job requirements;
3. Sensitivity of the components;
4. The period and/or frequency of removal.

C. LAC+USC Information Technology Management must document all requests and decisions concerning removal of any hardware and software.

D. LAC+USC Information Technology Management must update the hardware and software inventory system for both the removal and return of any hardware and software.

E. LAC+USC Information Technology Management must inspect any hardware and software upon its return to LAC+USC including a scan for malicious software.

F. LAC+USC Information Technology Management must provide an accounting of all documentation to the LAC+USC CIO at the time of the removal and return of the hardware and/or software.

### III. Data Backup

A. LAC+USC Information Technology Management must determine when backups are required before the movement of any hardware and software.

B. If a backup is created, it will be made in accordance with the data backup processes in the LAC+USC MC Policy No. 935.07, LAC+USC Information Technology (IT) Contingency Plan.

C. Any backup created must be tested to ensure that the copy is exact and is retrievable.

D. Any backup created must be stored in a secure location with appropriate access controls in place.

### IV. Disposal of hardware and software

A. LAC+USC Information Technology Management must ensure the hardware and software inventory system is appropriately updated upon the disposal of the hardware and/or software.

B. Before disposal, the Information Technology Management must ensure all PHI and other confidential and/or sensitive information on any component is irreversibly destroyed. The Information Technology Management must verify and document that the sanitization steps have been completed.

C. LAC+USC Information Technology Management must remove any labeling that had been affixed to the component before its disposal and affix it to the disposal documents.

D. LAC+USC Information Technology Management must provide an accounting of all documentation to the LAC+USC CIO at the time of the sanitization of the hardware and/or software.

E. LAC+USC Information Technology Management must submit written documentation with the disposal documents to verify that the sanitization steps were completed.

### V. Re-use of Devices and Media

A. LAC+USC Information Technology Management must ensure that the hardware and software inventory system is appropriately updated upon the reallocation of components.

B. Prior to re-use, LAC+USC Information Technology Management must ensure all information on any component is irreversibly destroyed. The Information Technology Management must verify and document that the sanitization steps have been completed.

### VI. Accountability

A. LAC+USC Information Technology Management must maintain a record of the movement of hardware, software, electronic media and devices and the persons responsible for those components.
B. LAC+USC may use existing inventory systems to collect the information required by this procedure. In the absence of an inventory system, LAC+USC must develop appropriate systems to collect the required information.

C. LAC+USC Information Technology Management must ensure that the hardware and software inventory system is up-to-date and secured.

## AUTHORITY

45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.310(d)(1) and (2)
Board of Supervisors Policy 6.101, Use of County Information Technology
DHS Policy No. 935.07, Facility Information Technology (IT) Contingency Plan

## CROSSREFERENCE

DHS Policies:
Network Policy No. 467, Information Technology (IT) Contingency Plan
DHS Policy No. 935.07, Facility Information Technology (IT) Contingency Plan

## REVISION DATES

February 11, 2014; September 22, 2017; October 30, 2020