LAC+USC MEDICAL CENTER POLICY

Page 1	Of 7

Subject: **WORKSTATION AND MOBILE DEVICE USE AND SECURITY**	Original Issue Date: 5/10/05	Policy # **458**
	Supersedes: 9/22/17	Effective Date: 10/30/20

Departments Consulted: Information Systems Health Information Management	Reviewed & Approved by: Attending Staff Associations Executive Committee Senior Executive Council	Approved by: (Signature on File) Chief Medical Officer (Signature on File) Chief Executive Officer

PURPOSE

To restrict workstation, use and access to Protected Health Information (PHI) and other confidential information by using physical, administrative, and technical controls.

POLICY

1. LAC+USC must ensure workstation security procedures are enforced within LAC+USC. “Workstations” include County and personal computers, mobile devices (e.g., tablet PCs, laptops, PDAs, computer carts), modems, printers, and fax machines, etc. that are used for County business.

2. All users must use workstations in a manner commensurate with the sensitivity of the Information accessed from the workstations.

3. All users must take reasonable physical security precautions to prevent unauthorized physical access to sensitive information from workstations. These precautions include taking into consideration the physical attributes of the surroundings (e.g., concealing video displays and securing unattended workstations).

4. LAC+USC Information Technology Management must implement physical safeguards to permit only authorized user access to workstations with accessibility to confidential and/or sensitive information.

5. Only LAC+USC supplied and supported workstations and mobile devices may be connected to LAC+USC Systems and access LAC+USC data. Exceptions to this may include remote access required by authorized vendors and business partners for support purposes.

6. LAC+USC DHS Enterprise Help Desk must implement a process to make positive identification of individuals requesting password resets due to forgotten passwords

   All users of workstations as described above must be trained to exercise proper security practices. Training and documentation must be in accordance with the LAC+USC Policy No. 120, LAC+USC Privacy and Security Compliance Program policies and procedures, including LAC+USC Policy No. 54401, Privacy and Security Training Policy, and LAC+USC Policy No. 479, Data Security Documentation Requirement.

PROCEDURE

LAC+USC CIO/designee must ensure that the following workstation security procedures are implemented within LAC+USC. “Workstations” include County and personal computers, mobile devices (e.g., tablet PCs, PDAs, computer carts), modems, printers, fax machines, etc., that are used for County business.

I. **Workstation Use**

These procedures are intended to include documented instructions delineating the proper functions to be performed by LAC+USC workforce members and the manner in which those functions are to be performed (e.g., logging off before leaving a workstation unattended) to maximize the security of health information.

Access and Use of Workstation and Network Services Measures to limit unauthorized access must include the following:

A. Configuration of workstations and network services.

1. LAC+USC Information Technology Management must configure workstations and network services to allow only authorized access to the workstation and network services (e.g., data, applications, intranet and Internet).

2. Workforce members must have authorization to access a workstation and the appropriate rights to do so. Users must not access any confidential and/or sensitive information from a workstation unless they have authorization to do so and it is necessary for doing their job.

B. Permitting only authorized access to workstations and network services through the use of controls.

LAC+USC CIO/designee, taking into consideration each system’s Risk Analysis Sensitivity Score, LAC+USC Policy No. 461, Security Management Process: Risk Management, is responsible for the creation, design and implementation of measures to limit unauthorized access by workforce members-to workstations and network services.

a. Unique User IDs and Passwords

i. The Facility CIO/designee is responsible for ensuring the assignment of a unique user ID to each User, to identify and track the User’s identity when logging into workstations, networks or applications.

ii. Each User must protect his/her password. Users must not write down their password and place it at or near the workstation (e.g., a note taped to the monitor or placed under the keyboard).

iii. Logging into workstations, networks or applications with another User’s ID and/or password is prohibited.

iv. Users must not share their unique User IDs (logon/system identifier) with any other person.

v. Users' passwords must be changed at least once every ninety (90) days.

vi. Passwords must be at least eight (8) characters and contain a combination of alpha and numeric characters.

vii. Two-factor authentication in which the User provides two means of identification, one of which is typically a physical token (e.g., a card), and the other of which is typically something memorized, (e.g., a security code) must be used when recommended in the Facility Master Security Management Report. (Refer to LAC+USC Policy No. 461, Security Management Process: Risk Management).

b. Other User Authentication Methods

With authorization from the DHS Departmental Information Security Officer (DISO), Facility CIOs may utilize other User authentication methods (e.g., badge readers, biometric devices, tokens).

c. Password Reset Requests (forgotten passwords)

Some form of personal information must be used to positively identify a user prior to executing a password reset request (e.g., ID badge, online challenge question, preset PIN, etc.).

C. Access to Workstations Not in Use

1. Workstations not in use must be password protected and locked.

2. Workstations must be setup to generate a screen saver when the computer receives no input for a specified period of time (to be determined by LAC+USC CIO based on result of risk assessment). Other "lockout" schemes that protect against the unauthorized access to confidential and/or sensitive information may be approved by the Facility CIO/designee.

D. Workstations must display an appropriate warning banner prior to gaining operating system access.

II. Access and Use of Mobile Devices

A. All mobile devices connected to LAC+USC systems or accessing LAC+USC data must be supplied and managed by LAC+USC IT departments. The applicable technical support group at LAC+USC will manage the maintenance of all Mobile Devices that connect to the LAC+USC networks.

B. Workforce members must exercise good judgment in determining the amount of necessary data stored on their mobile devices to perform their functions, as the security risk to such data is increased.

C. Access to mobile devices must be protected at all times consistent with the procedures set forth in the Access and Use of Workstation and Network Services section above.

D. Mobile devices containing sensitive information (e.g., confidential patient information) must be encrypted.

E. Use of personal USB drives (aka thumb drives) or other removable storage devices will be limited to read-only access while connected to a LAC+USC workstation. To ensure proper data security, only LAC+USC standard issued USB drives that are encrypted will be permitted read/write access while connected to a LAC+USC workstation. The only exception to this policy may be in the case that LAC+USC IT has approved and implemented security features on a workstation to ensure the adequate encryption of any personal USB drive device that may be connected to the workstation.

F. When traveling, a workforce member must not leave mobile devices unattended in non-secure areas.

G. Mobile devices that are left in cars must be stored out-of-sight and the car must be locked.

III. Physical Attributes of Surroundings

Workforce members must be aware of the physical attributes of the surroundings where the workstation is located. Precautions need to be taken to prevent unauthorized access to unattended workstations; to automatically erase sensitive information left displayed on unattended workstations; and to limit the ability of an unauthorized individual to observe sensitive information when a workstation is in use by a User. The following measures must be taken:

A. Confidential data (e.g., patient information) must be password protected, encrypted or stored on a secure network drive.

B. Confidential data having a Sensitivity Score of “High” must be encrypted.

C. Confidential data must not be downloaded without authorization from the Facility CIO/designee.

D. Confidential data must not be saved on removable devices (e.g., CD-ROM, external drives, USB drives) without proper safeguards and authorization from the Facility CIO/designee.

E. Removable media containing confidential data (e.g., patient information) must be maintained and stored in secured areas.

F. Printers are not to be left unattended in non-secure areas when printing confidential and/or sensitive information.

G. Disposal of confidential electronic records stored on removable or external media (e.g., CD-ROM, USB flash drives and removable hard drives) must be in accordance with LAC+USC Policy No. 473, Device and Media Controls

H. Use caution when viewing and entering confidential information.

I. Layout and design of the space must shield the view of the workstation screen from the public, unless the requirements of subsection III.J, below, apply and are complied with.

J. Where it is not possible, through layout and design of the space, to shield the workstation screen from view, devices like privacy screens and shields are to be used.

IV. Workstation Security

These procedures are intended to put in place physical safeguards to restrict access to information through securing LAC+USC workstations and laptops.

A. General

1. Workstations located in public or open areas must be physically secured in a locked room, locked cabinets, or strongly anchored to deter unauthorized movement. Security cameras or additional forms of monitoring should be considered in high-risk areas.

2. Users are required to secure laptop computers with a cable lock if the system is maintained or left in an insecure location. Additionally, users are required to adequately secure and monitor laptops while in transit (e.g., airports, in vehicles, etc.).

3. Mobile devices must be secured when not in use. These devices must either be carried on persons or must be stored in secured areas.

4. Workstation equipment must not be removed from the premises unless documented and pre-approved by the User’s supervisor.

5. Devices must be located in environments that are in accordance with the equipment manufacturer’s operational specifications.

6. Inventory and maintenance records must be maintained for all workstations.

7. Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation in accordance with LAC+USC Policy No. 492, Safeguards for Protected Health Information (PHI).

B. Hardware/Software

1. Workstations must be configured to require authentication (e.g., user ID and password) prior to users accessing system functions or data.

2. Workstations must be configured to store data to the network by default, as opposed to the user's local hard drive. Any sensitive data (e.g., ePHI) that must be stored locally on a mobile device must be approved and documented by LAC+USC management.

3. All mobile devices (e.g., tablets, laptops, PDAs, etc.) must be secured with full disk encryption to prevent disclosure of any data that maybe stored on the system.

4. Workstations settings must be configured to implement automatic screen locking after 30 minutes of inactivity. LAC+USC IT management approval and documentation is required where specific business processes call for longer periods for the inactivity setting.

5. Users are required to initiate the workstation screen-lock feature when stepping away from the system for short periods of time; users should log off for extended periods away from workstations. The screen-lock function is typically instituted by pressing the CTRL-ALT-DEL key sequence, then selecting “lock workstation.”

6. Personal firewalls must be enabled on all laptops. Laptops are commonly connected to non-LAC+USC networks (e.g., home networks, hotel networks, etc.) and thus, not protected by the security controls in place on the LAC+USC network. Personal firewalls will help ensure that laptops are not compromised while connected to non-LAC+USC networks.

7. Workforce members must not change the system configuration of their workstation without proper authorization (e.g., network properties, video card).

8. Workforce members must not install or uninstall software on their workstation without proper authorization and licensing (e.g., downloaded Internet software, games, patches, plug-ins, and screen savers).

9. Only authorized Users may install/uninstall software and perform repair services on workstations.

10. Workforce members-must not re-enable floppy drives, CD-ROM drives, USB ports, etc., on workstations that have access to confidential data, unless the workforce member is authorized to use those drives.

11. The Facility CIO/designee must ensure appropriate controls are in place when sending equipment off premises for maintenance (i.e., maintenance contract must include business associate language).

12. All hardware and software connected to LAC+USC network services must be managed centrally within LAC+USC.

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.

AUTHORITY

45 Code of Federal Regulations, Part 164, Subpart C, Section
164.310(a)(2)(iv)(b) and (c)
Board of Supervisors Policies:
6.100, Information Technology and Security Policy
6.101, Use of County Information Technology
6.102, Countywide Antivirus Security Policy
6.106, Physical Security

CROSS REFERENCES

DHS Policies:
361.23, Safeguards for Protected Health Information (PHI)
361.24, Privacy and Security Awareness and Training Policy
935.01, Security Management Process: Risk Management
935.13, Device and Media Controls
935.17, Person or Entity Authentication
935.19, Data Security Documentation Requirement
935.03, Workforce Security
935.14, System Access Control

REVISION DATES

May 13, 2005; October 03, 2008; February 11, 2014; September 22, 2017; October 30, 2020