LAC+USC MEDICAL CENTER POLICY

Subject: SYSTEM ACCESS CONTROL	Original Issue Date: 7/13/10	Policy # 474
	Supersedes: 9/22/17	Effective Date: 10/30/20

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

PURPOSE

To preserve and protect the confidentiality, integrity and availability of the LAC+USC, systems and applications, all access to the Information Technology Assets/Resources are permitted only to those persons or software programs that have been granted access rights.

POLICY

LAC+USC CIOs/designees must ensure that LAC+USC Information Technology Management implement the appropriate technical access control safeguards to allow LAC+USC electronic information systems access only to those persons or software programs that have been granted access rights:

1. Unique User Identification. LAC+USC systems must assign a unique name and/or number to each user for identifying and tracking user identity.

   Configure systems to track individual activity by user identification and record such activities as required by LAC+USC Policy No. 475, System Audit Controls.

2. System Log-in Banner. Every login process for multi-user computers must include a special notice. This notice must state:

   (1) the system is to be used only by authorized users, and
   (2) by continuing to use the system, the user represents that he/she is an authorized user.

3. System Log-in Monitoring. User and process access to system must be recorded and monitored for successful and failed attempts.

4. Emergency Access Procedure. LAC+USC systems must have alternate secured manual or automated procedures for accessing stored information during an emergency to be invoked by the Departmental Information Security Officer (DISO) or designee when the usual means of secured access is not available.

5. Automatic Logoff. LAC+USC CIOs/designees must ensure that the LAC+USC Information Technology Management address the use of an automated process to terminate an electronic session after a predetermined time of inactivity.

6. Encryption/Decryption. LAC+USC CIOs/designees must ensure that LAC+USC Information Technology Management address the appropriate encryption for protecting electronic information contained within the storage structure for all LAC+USC electronic data storage systems (i.e., databases or file systems) based on the LAC+USC Master Security Management Report in LAC+USC Policy 461, Information Security Management Process.

7. Information System Access Control Review and Documentation. Facility CIOs/designees, taking into consideration each system's Risk Analysis Sensitivity Score, must approve the design and implementation of controls to limit unauthorized access of workforce members to information systems including workstations, servers, networks, and applications.

LAC+USC Information Technology Management must document the implementation of the above safeguards in the System Security Implementation Plan that accompanies the electronic data system. The System Security Implementation Plan and all system documentation must be submitted to the DISO or designee for review.

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 164.308 (a)(3)(ii)

CROSS REFERENCES

DHS Policies:
935.01, Security Management Process: Risk Management
935.07, Facility Information Technology (IT) Contingency Plan
935.15, System Audit Controls
935.19, Data Security Documentation Requirement

REVISION DATES

July 13, 2010; February 11, 2014; September 22, 2017; October 30, 2020