Subject:	Original Issue Date:	Policy #
INFORMATION TECHNOLOGY FACILITY ACCESS CONTROL	7/13/10	**470**
	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 define the process for ensuring the physical protection of LAC+USCs' information systems and infrastructure.

POLICY

LAC+USC must implement policies and procedures to limit physical access to electronic information systems in which they are housed, while ensuring that properly authorized access is allowed. These policies and procedures must be consistent with LAC+USC Policy No. 120.1, Safeguards for Protected Health Information (PHI).

LAC+USC Access Control must include the following components to insure the integrity, confidentiality and availability of data:

1. Contingency Operations

LAC+USC must be responsible for developing, testing, implementing and maintaining the Information Technology (IT) component of LAC+USC Contingency Operations Plan that provides LAC+USC access when necessary to restore Information Systems and/or lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

2. LAC+USC IT Security Plan

LAC+USC must be responsible for developing, testing, implementing and maintaining the IT component of LAC+USC Security Plan to safeguard LAC+USC and the computer information assets therein from unauthorized physical access, tampering, and theft.

3. Physical Access Control and Validation (Personnel and Visitors)

LAC+USC must be responsible for developing, testing, implementing and maintaining the IT component of LAC+USC Access Control and Validation Procedure to control and validate each person's access to LAC+USC based on his/her role or function, including visitor control, and control of access to software programs for testing and revision.

4. LAC+USC Maintenance Records

LAC+USC must be responsible for developing, testing, implementing, and maintaining LAC+USC Security Maintenance Record to document repairs and modifications to the

physical components of LAC+USC that are related to security (e.g., hardware, walls, doors, and locks).

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

I. Contingency Operations

A. Identify systems and data and their location that, if lost, will be reestablished and/or restored as a part of LAC+USC disaster recovery plan or emergency mode of operation plan.

B. Identify the workforce members that need LAC+USC and/or system access in the event of a disaster or emergency.

C. Create and implement a backup authentication scheme to regulate LAC+USC access in the event of a disaster or emergency. Since electronic means cannot be relied upon during an emergency, a “manual” authentication scheme should also be developed.

D. When determining these access means, emergency communication means must be considered to ensure authorized access is granted in the event an obstacle is encountered.

E. The contingent access scheme must be tested periodically to ensure operational functionality.

F. These procedures must be coordinated with other LAC+USC contingency plan components including LAC+USC Policy No. 467, Facility Information Technology (IT) Contingency Plan.

II. LAC+USC Security Plan

The LAC+USC Security Plan is intended to limit physical access to LAC+USC’s electronic information systems and the areas in which they are housed. It is also intended to allow physical access to LAC+USC’s electronic information systems and the areas in which they are housed to workforce members who need access in furtherance of County business.

To accomplish this purpose, LAC+USC is taking a “layered approach.” This means that LAC+USC access measures will be “layered” – the more sensitive the area or system, the more restrictive the access control.

A. Exterior of Premises

The LAC+USC Security plan must:

1. Clearly define the security perimeter of the premises and buildings.

2. Ensure that the perimeter defined above is physically sound (i.e., no gaps in which a break-in is relatively easy).

3. Ensure that all external doors are adequately secured against unauthorized access by installing locks, alarms, or other access control devices.

4. Ensure that sensitive areas are monitored as necessary (e.g., video surveillance cameras with video recording capabilities).

5. Provide for a reception area (staffed at least during business hours in which visitors may access the building through a single entrance to the area).

6. Define the instances in which visitors are allowed, including the areas they visit and any escort requirements.

7. Ensure that any fire doors on the security perimeter are alarmed, have a self-closing mechanism, and are compliant with fire regulations.

8. If any of the measures in 1 through 7 above are determined to not be feasible, the plan must provide a justification and must ensure the security of the premises through other sufficient means.

B. Interior of Premises.
LAC+USC Security Plan must:

1. Ensure that any necessary physical barriers are extended from real floor to real ceiling.

2. Ensure that all doors to interior areas requiring compartmentalization or added security are adequately protected against unauthorized access by installing locks, alarms, or other access control devices.

3. Ensure that sensitive areas are monitored as necessary (e.g., video surveillance cameras with video recording capabilities).

4. Ensure that all doors and windows lock by default and that adequate security measures are in place for windows at ground level.

5. Intrusion detection systems are included where appropriate to provide additional security to interior premises and buildings.

6. Ensure that vacant secure areas are locked and periodically inspected.

7. If any of the measures in 1 through 6 above are determined to not be feasible, the plan must provide a justification and must ensure the security of the premises through other sufficient means.

C. LAC+USC Equipment
The LAC+USC Security Plan must:

1. Ensure that LAC+USC equipment requiring additional levels of protection be isolated from other equipment to the extent possible.

2. Position workstations such that monitor screens and keyboards are not directly visible to unauthorized persons.

3. Provide controls to guard against equipment theft such as closed-circuit television monitoring devices, alarms, locks, and controlled access.

4. Provide controls to guard against fire damage, such as smoke detectors, fire alarms and fire extinguishers as reasonable to protect the electronic information system.

5. Provide controls to guard against water damage, such as elevating workstations and other equipment as reasonable to protect the electronic information system.

6. Provide controls to ensure air quality is maintained that is appropriate for the equipment such as air conditioning, heating, dust filters, and air dehumidifiers/humidifiers, as reasonable to protect the electronic information system.

7. Provide controls to guard against damage caused by vibrations or electrical supply interference.

8. Provide controls to guard against power surges and outages, such as multiple power feeds, backup generators, and uninterruptible power supplies.

9. If any of the measures in 1 through 8 above are determined to not be feasible, the plan must provide a justification and must ensure the security of the information through other sufficient means.

III. Access Control and Validation
LAC+USC CIO/designee must ensure that the Information Technology Management and/or LAC+USC Managers:

A. Configure LAC+USC access controls to allow workforce members access based on the latest approved access rights and privileges.

B. Include a means to update LAC+USC access control settings to reflect workforce member status changes.

C. Ensure that visitors sign in upon entering LAC+USC.

D. Ensure that visitors are escorted by appropriate personnel where required by the LAC+USC Security Plan.

E. Ensure that workforce members testing and/or revising software programs are identified, authenticated and authorized to perform those activities.

IV. Maintenance Records

LAC+USC CIO/designee must:

A. Identify the physical components of LAC+USC that are relevant to IT security (e.g., hardware, walls, electronic systems, doors and locks).

B. Approve and oversee any IT security-related physical modifications to LAC+USC.

C. Create a maintenance record or log and ensure that it is updated for each such modification.

D. Ensure proper chain-of-custody for pertinent items like keys and access codes.

AUTHORITY

45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.310(a)(1) and (a)(2)(i-iv)
Board of Supervisors Policy 6.106, Physical Security

CROSS REFERENCE

DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI)

REVISION DATES

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