LAC+USC MEDICAL CENTER POLICY

		Page 1 Of 3
Subject: **SYSTEM AUDIT CONTROLS**	Original Issue Date: 7/13/10	Policy # **475**
	Supersedes: 9/22/17	Effective Date: 10/30/20
Departments Consulted: Information Systems Office of Human Resources	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 ensure audit control mechanisms that record and examine system activity are in place for all departmental electronic information systems.

POLICY

LAC+USC must ensure that data systems containing Protected Health Information (PHI) and other confidential information utilize a mechanism to log and store system activity in accordance with the recommended safeguards specified in the LAC+USC Master Security Management Report, LAC+USC Policy No. 461, Security Management Process: Risk Management.

LAC+USC must develop an Audit Control and Review Plan that describes the systems and applications to be logged, activities to be audited, responsibilities of workforce members involved in the implementation of the plan (including separation of duties), frequency of audits and the audit reporting and review process. The Plan must be reviewed and approved by the Departmental Information Security Officer (DISO) or designee.

LAC+USC must protect the confidentiality, availability and integrity of audit trails and internal audit reports.

LAC+USC must ensure that audit trails are backed up and that the backups are verified and tested to assure complete restoration capability.

PROCEDURE

LAC+USC CIO must ensure that LAC+USC Information Technology Management complete the Audit Control and Review plan as part of the System Security Documentation (LAC+USC Policy No. 474, System Access Control).

I. AUDIT CONTROL AND REVIEW PLAN

A. LAC+USC CIO must identify the components of the Facility's information systems environment that will record audit trails and be used in the internal audit process in the Audit Control and Review Plan. These components may include perimeter devices (e.g., firewalls, network intrusion detection systems, routers, switches, VPN appliances, and guard devices), servers (e.g., web, application, file, print and database), workstations and applications.

B. LAC+USC Information Technology Management must:

1. Define the events to be audited for the information system components identified above (e.g., logins, file access and data modification).
2. Determine the scope of the information that is to be recorded for both information at rest (storage) and information in transit (transmission).
3. Enable the auditing mechanism on the information system identified in I. A. above.
4. Determine the roles and responsibilities of workforce members for the operation of the auditing mechanism and the review of the audit reports. The monitoring and review of audit trails and internal audit reports must be assigned to a person who does not have responsibility for system operations.
5. Determine the frequency and content of audit reporting.
6. Escalate potential security incidents or unusual logged events to the Facility CIO/designee.

II. MANAGING THE SECURITY OF AUDIT TRAILS

LAC+USC Information Technology Management must maintain reasonable safeguards to ensure the confidentiality, availability, and integrity of audit trails and internal reports and to prevent unauthorized access. These safeguards must include, but not be limited to, the following:

A. Password protected access to audit logs and internal audit reports, including the use of file integrity checkers.

B. Regularly backing up audit logs and storing them in fire resistant, offsite, locked containers. The process of audit trails and internal audit reports must be consistent with the data backup procedures in LAC+USC Policy No. 467, LAC+USC Information Technology (IT) Contingency Plan.

C. Limiting the number of persons necessary for monitoring and reviewing audit trails and internal audit reports.

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 (CFR) Part 164, $164.132(b)
Board of Supervisors Policy:
6.107, Information Technology Risk Assessment
6.108, Auditing and Compliance

CROSS REFERENCES

DHS Policies:
935.01, Security Management Process: Risk Management

935.07, Facility Information Technology (IT) Contingency Plan
935.14, System Access Control

REVISION DATES

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