LAC+USC MEDICAL CENTER POLICY

Subject: **LAC+USC INFORMATION TECHNOLOGY AND SECURITY POLICY**	Original Issue Date: 5/13/05	Policy # **460**
	Supersedes: 9/22/17	Effective Date: 10/30/20

Departments Consulted:	Reviewed & Approved by:	Approved by:
Information Systems Risk Management Office of Human Resources	Attending Staff Association Executive Committee Senior Executive Council	(Signature on File) Chief Medical Officer (Signature on File) Chief Executive Officer

PURPOSE

The purpose of this policy is to provide direction for the development and implementation of data security policies and procedures and to identify the data security officials and their responsibilities.

POLICY

LAC+USC Medical Center is responsible for securing all electronic data, including Protected Health Information (PHI) and other confidential information, while complying with the security requirements of all applicable regulatory, compliance and accreditation sources, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Medicare, Medi-Cal and JCAHO.

The term PHI, as used in the DHS Information Technology (IT) security policies 935 series, refers to electronic Protected Health Information.

LAC+USC must develop data security policies and procedures to ensure the security of PHI and other confidential information, and the hardware and systems used to obtain, utilize, and maintain such information.

All LAC+USC workforce members must comply with provisions of the LAC+USC data security policies. Any workforce member who fails to comply will be subject to disciplinary action in accordance with DHS Policy No. 361.10, Disciplinary Action for Failure to Comply with Privacy Policies and Procedures, DHS Policy No. 747, Disciplinary Action, Civil Service Rule 18.031 and the DHS Employee Evaluation and Discipline Guidelines.

To ensure compliance with the provisions of this policy, the following responsibilities have been designated to the following data security officials:

I. Departmental Information Security Officer (DISO)

A. LAC+USC must designate a DISO who is responsible for the development, implementation and maintenance of LAC+USC data security policies, procedures and guidelines.
B. The DISO will assist LAC+USC managers in the risk analysis and management process.
C. The duties of the DISO include, but are not limited to the following:

1. Chair the Departmental Information Security Steering Committee (DISSC).
2. Provide information security related technical, regulatory, and policy leadership.

3. Facilitate the development and implementation of the LAC+USC information security policies and procedures.
4. Coordinate information security efforts across the facility in alignment with DHS and Countywide security policies.
5. Direct continuing information security training and education efforts.
6. Represent LAC+USC at the County Information Security Steering Committee (ISSC).
7. Report to the LAC+USC Chief Information Officer (CIO) and DHS Chief Information Security Officer (CISO).
8. Ensure LAC+USC is in compliance with all laws, rules and regulations as it relates to the proper handling of data and electronic media.
9. Recommend new security standards as technology changes.
10. Coordinate LAC+USC and DHS enterprise security software and hardware purchasing and licensing.
11. Review and approve data security implementation and risk management efforts.

D. The DISO or designee must review and approve the Risk Analysis Report.
E. The DISO or designee must review and approve the LAC+USC Facility Master Security Management Report, LAC+USC Policy No. 461, Security Management Process: Risk Management.
F. The DISO must assist LAC+USC facility Information Technology management in implementing the access authorization procedures and determining the appropriate technical access controls.
G. The DISO or designee will coordinate the Departmental Computer Emergency Response Team (DCERT).
H. The DISO or designee and DCERT are responsible for determining the appropriate level of response to a security incident.
I. The DISO or designee must represent the department at the County Computer Emergency Response Team (CCERT) as the primary department CERT member (DCERT).

II. LAC+USC Chief Information Officer (CIO)

The duties of the LAC+USC CIO or designee must include:

A. Management responsibility over all systems within LAC+USC.
B. Ensure that LAC+USC System Managers/Owners conduct risk assessments for their data resources and information systems in accordance with LAC+USC procedures.
C. Create and periodically update the LAC+USC Master Security Management Report.
D. Ensure that LAC+USC System Managers/Owners develop plans to implement the LAC+USC Master Security Management Report's recommended safeguards and actions.
E. Ensure that LAC+USC System Managers/Owners establish, document, and implement procedures for reviewing information systems activity, including but not limited to audit logs, problem logs, system access reports, change control logs, and security incident reports.
F. Work with LAC+USC System Managers/Owners, LAC+USC Information Technology management and LAC+USC Human Resources to develop workforce security procedures and to coordinate those activities necessary to implement the workforce security procedures.

G. Ensure that LAC+USC Information Technology management authorize access to information resources under their control on a "need to know basis" for carrying out the essential job functions of the workforce members.
H. Ensure that LAC+USC Information Technology management implement procedures for establishing LAC+USC workforce member access to electronic information, for example, through access to a workstation, transaction, program, process, or other mechanism, that is both necessary and appropriate for the job functions of the workforce member.
I. Ensure that LAC+USC Information Technology management implement procedures that modify a user's right of access to a workstation, transaction, program, process, or other mechanism, when such modification is necessary to align the workforce members' access with the workforce members' essential job functions.
J. Ensure that the LAC+USC Information Technology management respond to security incidents and emergency situations in a manner authorized and directed by the DISO or designee and DCERT.

III. LAC+USC System Managers/Owners

LAC+USC Information Technology management security responsibilities include, but are not limited to, the following:

A. Establish rules for system use and protection of the PHI and other confidential information as required in LAC+USC Policy No. 120 LAC+USC Privacy and Security Compliance Program policy.
B. Work with LAC+USC CIO to develop and implement the LAC+USC Policy No. 461, Security Management Process: Risk Management.
C. Establish, document, and implement procedures for reviewing information systems activity, including but not limited to audit logs, problem logs, system access reports, change control logs, and security incident reports.
D. Work with LAC+USC CIO or designee, LAC+USC managers and supervisors and LAC+USC Human Resources to develop workforce security procedures and to coordinate those activities necessary to implement the workforce security procedures.
E. Implement procedures for establishing LAC+USC workforce member access to electronic information, for example, through access to a workstation, transaction, program, process, or other mechanism, that is both necessary and appropriate for the job functions of the workforce member.
F. Ensure that each workforce member with access has signed an acknowledgment of LAC+USC Policy No. 480, Acceptable Use Policy for County Information Technology Resources that defines their responsibility for protecting the confidentiality, integrity and availability of all DHS and LAC+USC information resources and identifying restrictions for utilizing those resources.
G. Determine the sensitivity and criticality of the resources for which they are responsible and develop, implement and maintain the Contingency Plan (CP) commensurate with the criticality.
H. Ensure that appropriate physical safeguards and technical security policies are implemented.
I. Define the system's security requirements in a System Security Documentation.
J. Train and communicate to the workforce member the proper procedures for protecting the PHI and other confidential information.

IV. LAC+USC **Human Resources (HR)**

The security responsibilities of the LAC+USC Human Resources must include:

A. Work with DHS Human Resources to ensure proper workforce clearance procedures are implemented. Refer to DHS Policy No. 703.1, Criminal Records Background Check/ Fingerprinting Policy.
B. Ensure that each new workforce member receives and signs acknowledgment of LAC+USC Policy No. 480, LAC+USC Acceptable Use Policy for County Information Technology Resources during the new hire orientation and that each workforce member completes the acknowledgment during the annual Performance Evaluation process. Signed acknowledgments will be filed in the workforce member's official personnel folder.

V. Workforce Managers and Supervisors

The security responsibilities of workforce managers and supervisors must include:

A. Determine workforce members' access rights and levels based on the workforce members' job responsibilities and authorize workforce members' access to electronic data systems, the Internet and Intranet systems.
B. Supervise the activities of LAC+USC workforce members in relation to the use and disclosure electronic data.
C. Identify and supervise workforce members who work with confidential and/or sensitive information or who work in locations where confidential and/or sensitive information might be accessed.
D. Provide authorization and supervision to workforce members and others who need to be in areas where confidential and sensitive information may be accessed and take appropriate safeguards to ensure those who may be exposed to confidential or sensitive information are made aware of the policies protecting that information.

VI. Workforce Member

The security responsibilities of all LAC+USC workforce members must include:

A. Compliance with the provisions of all relevant data security policies and procedures. Including but not limited to LAC+USC Policy No. 120, Privacy and Security Compliance Program, LAC+USC Policy No. 457, Acceptable Use Policy for County Information Technology Resources, and LAC+USC Policy No. 458, Workstation Use and Security.
B. Report any and all suspected and actual breaches of information security to the LAC+USC DISO.

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, §164.308(a)(2)
Health Insurance Portability and Accountability Act of 1996 (HIPAA) Public Law 104-91
Board of Supervisor's Policy Nos. 6.100 Information Technology and Security Policy

CROSS REFERENCES

Board of Supervisor's Policy Nos.
6.101 Use of County Information Technology Resources
6.102 Countywide Antivirus Security Policy
6.103 Countywide Computer Security Threat Response
6.104 Use of Electronic Mail (e-mail) by County Employees
6.105 Internet Usage Policy
6.106 Physical Security
6.107 Information Technology Risk Assessment
6.108 Auditing and Compliance
DHS Policy No. 183, Delegation of Information Resources Authority
361.1 Privacy and Security Compliance Program
935.01 Security Management Process: Risk Management
935.11 Workstation Use and Security
935.20 Acceptable Use Policy for County Information Technology Resources

ATTACHMENTS

Attachment A: DHS Information Security Glossary

REVISION DATES

May 13, 2005; October 03, 2008; July 13, 2010; February 11, 2014; September 22, 2017; October 30, 2020