Subject:	Original Issue Date:	Policy #
ACCEPTABLE USE POLICY FOR COUNTY INFORMATION TECHNOLOGY RESOURCES	5/10/05	**457**
	Supersedes: 9/22/17	Effective Date: 10/30/20

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

PURPOSE

To ensure LAC+USC workforce members follow acceptable use of County information technology resources within the department.

POLICY

Each LAC+USC workforce member is required to adhere to and management is expected to strictly enforce all policies and procedures with respect to the proper use of County information technology resources in accordance with LAC+USC Policy No. 120, LAC+USC Privacy and Security Compliance Program, the County Fiscal Manual, and other County and LAC+USC information technology use policies and procedures.

All workforce members are required to sign acknowledgment of the receipt and review of the County and LAC+USC's Acceptable Use policy (as noted below). LAC+USC Human Resources must ensure that each new hire or transferred County workforce member receives and signs the following documents during in-processing

1. *County of Los Angeles Agreement of Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data (County Acceptable Use Agreement)* and,

2. Acknowledgment of this policy

Managers/supervisors must review both documents and have them signed and completed by each County workforce member during the annual performance evaluation process.

Each Non-County workforce member shall receive and acknowledge the "LAC+USC Comprehensive Policy Statement" in accordance with the non-County workforce member in-processing procedures. The "LAC+USC Comprehensive Policy Statement" must also be provided to and acknowledged by the non-County workforce member in conjunction with their annual performance review process.

LAC+USC Information Technology Management will ensure that all workforce members with access to County information technology resources have signed the agreement and acknowledgment prior to providing access.

I. RESPONSIBILITY

Access to County information technology resources and accounts is a privilege granted to workforce members based on their job duties and may be modified or revoked at any time. Each workforce member is responsible for the protection of LAC+USC's information technology resources. Workforce members must protect all Information contained in the technology resources as required by local, state and federal laws and regulations. Each workforce member must sign and abide by the County Acceptable Use Agreement and the provisions of this policy.

County workforce members will be required to sign the County Acceptable Use Agreement and the acknowledgment at the time of new hire or transfer into LAC+USC and annually as part of the performance evaluation process. Non-County workforce members will be required to acknowledge the County Acceptable Use Agreement and this policy by signing the "LAC+USC Comprehensive Policy Statement" during the in-processing procedure and in conjunction with their annual performance review.

The completed acknowledgment forms must be filed in the workforce member's personnel folder. Acknowledgments from the "LAC+USC Comprehensive Policy Statement" will be filed in the non-County workforce member's Human Resources file.

Violation of the County Acceptable Use Agreement or this policy may result in disciplinary action, up to and including, discharge and possible civil and/or criminal liability.

Non-County workforce members found to be in violation of the County Acceptable Use Agreement or this policy may be released from assignment and recorded as a "do not send" in the LAC+USC "Do Not Send" Database.

The County information technology resources are the property of the County and are to be used for authorized business purposes only.

II. WORKFORCE MEMBER PRIVACY

Workforce members have no expectation of privacy with respect to their use of the County information system assets, because at any time LAC+USC may log, review, or monitor any data created, stored, accessed, sent, or received. LAC+USC has, and will exercise, the right to monitor any information stored on a workstation, server or other storage device; monitor any data or information transmitted through the LAC+USC Medical Center; and/or monitor sites visited on the LAC+USC Intranet, Internet, chat groups, newsgroups, material downloaded or uploaded from the Internet, and e-mail sent and received by workforce members. Activities, communications, or computer usage not related to County business are likely to be monitored. LAC+USC may use manual or automated means to monitor use of its County information technology resources.

A supervisor/manager may request to review the system activities of a subordinate if misuse of LAC+USC system resources is suspected. If evidence of misuse of LAC+USC system resources is identified, the supervisor/manager must contact the LAC+USC Audit & Compliance Division to determine appropriate actions. The LAC+USC Audit & Compliance Division may also be required to contact the Auditor-Controller's Office of County Investigations.

Violations involving non-County workforce members shall be referred to the Facility Liaison/Contract Monitor for appropriate action.

Use of passwords to gain access to County information technology resources or to encode particular files or messages does not imply any expectation of privacy in the material created or received. The requirement for use of passwords is based on LAC+USC's obligation to properly administer information technology resources to ensure the confidentiality, integrity and availability of Information. Workforce members are required to authenticate with a unique Employee/Workforce member ID so that all access may be auditable.

III. PROHIBITED ACTIVITIES

A. Prohibited Uses: Workforce members are prohibited from using County information technology resources for any of the following activities:

1. Engaging in unlawful or malicious activities.
2. Sending, receiving or accessing pornographic materials.
3. Engaging in abusive, threatening, profane, racist, sexist or otherwise objectionable language.
4. Misrepresenting oneself or the County.
5. Misrepresenting a personal opinion as an official County position.
6. Defeating or attempting to defeat security restrictions on County systems or applications.
7. Engaging in personal or commercial activities for profit.
8. Sending any non-work related messages.
9. Broadcasting unsolicited, non-work related messages (spamming).
10. Intentionally disseminating any destructive program (e.g., viruses).

11. Playing games or accessing non-business related applications, or social networking sites.

12. Creating unnecessary or unauthorized network traffic that interferes with the efficient use of County information technology resources (e.g., spending excessive amounts of time on the Internet, engaging in online chat groups, listening to online radio stations, online shopping).

13. Attempting to view and/or use another person's accounts, computer files, program, or data without authorization.

14. Using County information technology resources to gain unauthorized access to LAC+USC or other systems.

15. Using unauthorized wired or wireless connections to LAC+USC networks.

16. Copying, downloading, storing, sharing, installing or distributing movies, music, and other materials currently protected by copyright, except as clearly permitted by licensing agreements or fair use laws.

17. Using County information technology resources to commit acts that violate state, federal and international laws, including but not limited to laws governing intellectual property.

18. Participating in activities that may reasonably be construed as a violation of National/Homeland security.

19. Posting scams such as pyramid schemes and make-money-quick schemes.

20. Posting or transmitting private, proprietary, or confidential information, including patient information, to unauthorized persons, or without authorization.

21. Downloading confidential or patient information or data onto a mobile storage device without authorization from the Facility CIO/designee.

22. Using Online Web-based Document Sharing Services (e.g., Google Docs, Microsoft Office Live, Open-Office) to store or share LAC+USC data.

23. Viewing, accessing, using or disclosing confidential or patient information or data if not authorized as part of the workforce member's job duties.

B. Misuse of software: Workforce members must not engage in software copyright infringements. Workforce members are prohibited from conducting the following activities without proper licensing and prior written authorization by the Facility CIO/designee:

1. Copying County-owned software onto their home computers.
2. Providing copies of County-owned software to independent contractors, clients or any other third-party person.
3. Installing software on any LAC+USC workstation (e.g., desktops, personal computers, mobile devices, and laptop) or server, unless authorized by their supervisors and IT management.
4. Downloading software from the Internet or other online server to LAC+USC workstations or servers.
5. Modifying, revising, transforming, recasting or adapting County-owned software.
6. Reverse-engineering, disassembling or decompiling County-owned software.

IV. PASSWORDS

Workforce members are responsible for safeguarding their passwords for access to the County information technology resources. Workforce members are responsible for all transactions made using their passwords. Workforce members may not provide their password or use their password to provide access to another Workforce member; or access the County information technology resource with another Workforce member's password or account. Some systems have a universal access password with a secondary password neither of which shall be shared with workforce members who are not authorized to utilize the system. Workforce members should be aware that leaving a computer unattended for a brief time, even 30 seconds, may give an unauthorized user enough time to access the system using the previous user's access.

V. SECURITY

A. County information technology resources

Workforce members are responsible for ensuring that the use of outside computers and networks, such as the Internet, do not compromise the security of County information technology resources. This responsibility includes taking reasonable precautions to prevent intruders from accessing County information technology resources.

B. Malicious software

Malicious software can cause substantial damage or inconvenience to County information technology resources. Workforce members are responsible for taking reasonable precautions to ensure that they do not introduce malicious software into County information technology resources. Workforce members must not bypass or disable County malicious software protections. Workforce members must only use or distribute storage media or e-mail (including attachments) known to the workforce member to be free from malicious software.
Any workforce member who telecommutes or is granted remote access must utilize equipment that contains current County-approved anti-virus software and must adhere to

County hardware/software protection standards and procedures that are defined by the County and the authorizing Department.

LAC+USC restricts access to the Internet or any other network via modem, cellular wireless, or other telecommunication services. No workforce member may employ any external inbound or outbound connections to LAC+USC network resources unless explicitly authorized by the Departmental Information Security Officer (DISO) or designee.

Each workforce member is responsible for notifying the DHS Enterprise Help Desk or the Departmental Information Security Officer as soon as a device is suspected of being compromised by a virus.

VI. E-MAIL

Access to County e-mail services is a privilege that may be wholly or partially restricted without prior notice and without consent of the workforce member. E-mail messages are the property of the County and subject to review by authorized County personnel.

E-mail messages are legal documents. Statements must not be made on e-mail that would not be appropriate in a formal memo. Workforce members must endeavor to make each electronic communication truthful and accurate. Workforce members are to delete e-mail messages routinely in accordance with both the LAC+USC and County E-mail policies**.**

Protected Health Information (PHI) and other confidential and/or sensitive information can only be sent or received if it is encrypted or safeguarded in accordance with DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI).

Access to Internet-based e-mail sites (e.g., Yahoo Mail, Google Mail, Hotmail, etc.) is not permitted. Exceptions to this policy must be based upon requirements to perform job-related activities and be approved by LAC+USC management.

Default E-Mail Retention Period

LAC+USC e-mail systems will be configured to **automatically delete** messages greater than **three years** on active e-mail servers. This auto-delete policy applies to messages within all folders (inbox folders, sent file folders, draft file folders, etc.) stored on active e-mail servers. LAC+USC will have three levels of e-mail users. (Level 1 is 3 years, Level 2 is 5 years, and Level 3 is 7 years of retention time)

All LAC+USC e-mail system users are expected to:

1. Regularly check for new messages;

2. Delete **transitory** messages as quickly as possible.

a. Specially defined groups will have a maximum of either a three or five year retention period.

b. Specially defined groups may consist of members from Audit and Compliance, Risk Management, Human Resources, Finance, and facility CEO's.

c. Facility CIO from defined groups will determine which individuals will be allowed a three or five year retention period.

d. No Personal Storage Table, (PST) files will be allowed or used by LAC+USC e-mail users.

e. E-mail is not to be used for the storage of patient/protected health information of any kind, nor is it to be used as a document storage system.

VII. USE OF THE INTERNET

Use of the Internet must be in accordance with LAC+USC and County Internet and privacy policies.

All LAC+USC Internet activities are monitored and audited by LAC+USC Security Operations and Compliance Divisions.

Unauthorized non-County business Instant Messaging and Streaming Media are strictly prohibited.

Workforce members must not allow another workforce member to access the Internet using their authorized account.

LAC+USC is not responsible for material viewed or downloaded by workforce members from the Internet. The Internet is a worldwide public network that is uncensored and contains sites that may be considered offensive. Workforce members accessing the Internet do so at their own risk and LAC+USC shall not be liable for inadvertent exposure to any offensive materials.

Internet access is provided to the workforce member at the discretion of LAC+USC.

VIII. INFORMATION TECHNOLOGY USER ACCOUNT MANAGEMENT

When a workforce member leaves the County service, Human Resources will disable the user account. The mailbox will remain enabled for 60 days. After 60 days, the Active Directory (AD) account will be deleted from the AD and the mailbox will be deprovisioned.

LAC+USC Information Technology Department shall adhere to this minimum standard/guideline.

LAC+USC Information Technology Department shall develop and implement procedures to ensure compliancy.

IX. RECORDABLE MOBILE DEVICES AND REMOVABLE MEDIA

Workforce members must manage and control all recordable mobile devices and removable media that contain PHI or other confidential information. These devices include PDA's, USB flash drives, personal cell phones, cameras, removable hard disks, CD-R, CD-RW, DVD-R, DVD-RW and floppy disks.

The use of recordable mobile devices and removable media must be pre-approved and registered for use by the Facility CIO/designee in accordance with LAC+USC Policy No. 458, Workstation Use and Security: Access and Use of Mobile Devices and LAC+USC Policy No. 935.13 Device and Media Controls: Accountability.

X. REMOTE ACCESS SERVICES

No workforce member may employ any remote inbound or outbound connections to LAC+USC resources unless explicitly authorized by the Departmental Information Security Officer (DISO) or designee.

Unauthorized Remote Access Services (e.g., LogMeIn, GoToMyPC) are strictly prohibited.

Any workforce member who is granted remote access to the LAC+USC network must utilize the approved LAC+USC Information Security method for remote access. VPN and VDI are the LAC+USC approved remote access solutions until further notice.

Dial-up, DSL, modem etc. are strictly prohibited.

At no time should any workforce member share their remote access privileges with anyone, including other workforce members or family members.

DEFINITIONS

INFORMATION TECHNOLOGY RESOURCES/ASSETS
Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources.

INFORMATION TECHNOLOGY USER ACCOUNTS
An authorized user account (i.e., E-mail, Internet, Network File Share, Health Information System, etc.) provided to a user, to be used solely by that user, for the purpose of accessing services as granted to that user account.

PERSONAL STORAGE TABLE
A file that stores e-mail messages, calendar events and contact information used in applications such as Microsoft Outlook.

REMOTE ACCESS SERVICE
A service that supports connecting a PC from a location outside of the LAC+USC Medical Center (e.g. home) to the LAC+USC Medical Center or vice versa.

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

Board of Supervisors Policies:
6.101, Use of County Information Technology Resources
6.102, Countywide Antivirus Security Policy
6.104, Use of Electronic Mail (E-mail) by County Employees
6.105, Internet Usage Policy

CROSS REFERENCES

DHS Policies:
361.1, DHS Privacy and Security Compliance Program
361.23, Safeguards for Protected Health Information (PHI)
935.00, DHS Information Technology and Security Policy
935.11, Workstation Use and Security
935.13, Device and Media Controls

ATTACHMENTS

Attachment A: Agreement for Acceptable Use (AAU)

REVISION DATES

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