

COUNTY OF LOS ANGELES

AGREEMENT FOR ACCEPTABLE USE AND CONFIDENTIALITY OF COUNTY'S INFORMATION TECHNOLOGY ASSETS, COMPUTERS, NETWORKS, SYSTEMS AND DATA

As a Los Angeles County, employee, contractor, vendor, or other authorized employee of County Information Technology (IT) assets including computers, networks, systems and data, I understand that I occupy a position of trust. I will use County IT assets for County management approved business purposes only and maintain the confidentiality of County's business and Citizen's private data. As an user of County's IT assets, I agree to the following:

1. Computer Crimes: I am aware of California Penal Code 502(c) – Comprehensive Computer Data Access and Fraud Act (attached). I will immediately report any suspected computer misuse or crimes to my Management.
2. Security Access Controls: I will not subvert or bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. I will not share my computer identification codes (log-in ID, computer access codes, account codes, ID's, etc.) or passwords.
3. Approved Business Purposes: I will use the County's Information Technology (IT) assets including computers, networks, systems and data for County management approved business purposes only.
4. Online Web-based Document Sharing Services
I will not use Online Web-based Document Sharing Services to collaborate with workforce members; to store and/or share DHS owned data.
5. UNAUTHORIZED APPLICATION OR SOFTWARE
I will not download, install, or use any non-DHS approved application or software, such as Instant Messaging, Streaming Media, and Remote Access Services (e.g., LogMeIn, GoToMyPC).
6. Confidentiality: I will **not view, access, use or disclose** any County program code, data, information or documentation to any individual or organization unless specifically authorized to do so by the recognized information owner.
7. Computer virus and malicious code: I will not intentionally introduce any computer virus, worms or malicious code into any County computer, network, system or data. I will not disable or delete computer virus detection and eradication software on County computers, servers and other computing devices I am responsible for.
8. Offensive materials: I will not access or send any offensive materials, e.g., sexually explicit, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.
9. Public Internet: I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services may be filtered but in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be exposed to such offensive materials. I understand that my Internet activities may be logged, are a public record, and are subject to audit and review by authorized individuals.
10. Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will comply with County and DHS e-mail use policy and use proper business etiquette when communicating over e-mail systems.

11. Copyrighted materials: I will not copy any licensed software or documentation except as permitted by the license agreement.
12. Passwords: **I understand that I am responsible for safeguarding my passwords for access to County information technology resources and am responsible for all transactions made using my password. I will not share my passwords or provide access to another individual using my password.**
13. Disciplinary action for non-compliance: I understand that my non-compliance with any portion of this Agreement may result in disciplinary action including my suspension, discharge, denial of service, and cancellation of contracts or both civil and criminal penalties.

**CALIFORNIA PENAL CODE 502(c)
“COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT”**

Below is a section of the “Comprehensive Computer Data Access and Fraud Act” as it pertains specifically to this Agreement. California Penal Code 502(c) is incorporated in its entirety into this Agreement by reference and all provisions of Penal Code 502(c) apply. For a complete copy, consult the Code directly at website www.leginfo.ca.gov/.

502. (c) Any person who commits any of the following acts is guilty of a public offense:

- (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongly control or obtain money, property, or data.
- (2) Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- (3) Knowingly and without permission uses or causes to be used computer services.
- (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
- (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.
- (9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system or computer network.

LAC+USC HEALTHCARE NETWORK SUPPLEMENT TO

Recordable Mobile Devices and Removable Media: All recordable mobile and removable media that contain Protected Health Information or sensitive business information covered by HIPAA, Civil Code 1798.29 & 1798.82, must be managed and controlled. These devices include PDA's, USB flash drives, cellular phone, cameras and camera phones, removable hard disks, CD-R, CD-RW, DVD-R, DVD-RW and floppy disks.

Management and Control: I understand all information protected under HIPAA, California Civil Codes 1798.29 and 1798.82 and other non-public business information stored and accessible on recordable mobile devices and/or recordable storage must be managed and controlled. The use of recordable mobile devices must be recognized by the Department Head. Recordable storage media must be managed and controlled through the use of auditable inventory logs.

Please list all the electronic devices, i.e. CDROM, PDA, USB, etc, you expect to utilize when accessing, recording, capturing, storing or transmitting information protected under HIPAA, California Civil Codes 1798.29 and 1798.82 and other non-public business information.

- 1. _____ 3. _____
- 2. _____ 4. _____

ACKNOWLEDGMENT:

I acknowledge that I have received and read the Department of Health Services' Policy No. 935.20, DHS (LAC+USC Policy No. 457) Acceptable Use Policy for County Information Technology Resources and the County of Los Angeles Agreement of Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data. I agree to abide by the provisions of the policy and the agreement. If I fail to comply with the policy and agreement, I will be subject to disciplinary action, up to and including discharge. If I have any questions concerning the policy or agreement, I will discuss them with my supervisor.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

_____	_____	_____	_____
Employee's Name	Employee's Signature	Ext.	Date

_____	_____	_____
Employee's Job Title	Employee Number	E-mail Address

_____	_____	_____	_____
Manager's Name	Manager's Signature	Ext.	Date

_____	_____
Location-Room Number	Department Name

After completing the form, please, fax it to the Information System office at **Fax# 323-441-8056.**

Distribution:

Original – Employee Official Personnel Folder
Duplicate – Retain in Departmental Area File for Personnel: employees, contractors, students, volunteers and agency personnel.