COUNTY OF LOS ANGELES
Public Health

SUBJECT:	ACCEPTABLE USE POLICY FOR COUNTY INFORMATION TECHNOLOGY RESOURCES	PAGE 1 OF 7
POLICY No.: 1016		**EFFECTIVE DATE:** 04/15/09
APPROVED BY: J E Fielding		**SUPERSEDES:** DHS Policy No. 935.20

PURPOSE: To ensure the proper use of County information technology resources within the Department of Public Health (Public Health).

POLICY: Proper use of County information technology resources must be adhered to by each User and strictly enforced by management in accordance with Public Health Policy No. 1201, Public Health Privacy and Security Compliance Program, the County Fiscal Manual, and other County and Public Health information technology use policies and procedures.

All Users are required to sign acknowledgment of the receipt and review of the County and Public Health's Acceptable Use policy (as noted below). Public Health Human Resources must ensure that each new User receives and signs the *County of Los Angeles Agreement for Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data* and, the *Acknowledgement of Public Health Policy 1016 Acceptable Use for County Information Technology Resources* during the new hire orientation (or, for vendors, before work begins) and that each User (except vendors) completes the agreement and acknowledgment during the annual Performance Evaluation process. The signed agreement and acknowledgment will be filed in the User's official personnel folder (or vendor file).

Public Health System Managers/Owners will ensure that all Users 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 are privileges granted to individual Users based on their job duties and may be modified or revoked at any time. Each User is responsible for the protection of Public Health's County information technology resources. Users must protect all Information contained in the technology resources as required by local, state and federal laws and regulations. Each User must sign and abide by the County Acceptable Use Agreement for County information technology assets and acknowledgment of this policy during the new hire orientation (or, for vendors, before work begins) and

(except for vendors) must complete the Agreement and Acknowledgment during the annual Performance Evaluation process. Both forms must be filed in the employee's official personnel folder (or vendor file). Violation of the County Agreement or this Acceptable Use Policy may result in disciplinary action, up to and including, discharge, and possible civil and/or criminal liability.

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 Public Health may log, review, or monitor any data created, stored, sent, or received. Public Health 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 Public Health network; and/or monitor sites visited on the Public Health Intranet, Internet, chat groups, newsgroups, material downloaded or uploaded from the Internet, and e-mail sent and received by workforce members. The kinds of information that will be obtained through the monitoring include any information from any Public Health computer system. Activities or communications or computer usage not related to County business are likely to be monitored. Public Health may use manual or automated means to monitor use of its County information technology resources.

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 Public Health's obligation to properly administer information technology resources to ensure the confidentiality, integrity and availability of Information. Users are required to authenticate with a unique User ID so that all access may be auditable.

III. PROHIBITED ACTIVITIES

A. Prohibited Uses: Users 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;

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);

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 Public Health's or other systems;

15. Using unauthorized wired or wireless connections to Public Health 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.

B. Misuse of software: At no time must Users be engaged in software copyright infringements. Users 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 Public Health workstation (e.g., desktops, personal computers, mobile devices, laptops) or server;

4. Downloading software from the Internet or other online server to Public Health workstations or servers;

5. Modifying, revising, transforming, recasting or adapting County-owned software;

6. Reverse-engineering, disassembling or decompiling County-owned software.

IV. PASSWORDS

Users are responsible for safeguarding their passwords for access to the County information technology resources. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the County information technology resource with another User's password or account, unless such access is explicitly allowed by the accessing User's job description.

V. SECURITY

A. County information technology resources

Users 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. Users are responsible for taking reasonable precautions to ensure that they do not introduce malicious software into County information technology resources. Users must not bypass or disable County malicious software protections. Users must only use or distribute storage media or e-mail (including attachments) known to the User to be free from malicious software.

Any User 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.

Public Health restricts access to the Internet or any other network via modem, DSL, cellular wireless, or other telecommunication services. No User may employ any external inbound or outbound connections to Public Health network resources unless explicit authorized by the DISO or designee.

Each User is responsible for notifying the Department's Help Desk or the Department Security contact 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 User. 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. Users must endeavor to make each electronic communication truthful and accurate. Users are to delete e-mail messages routinely in accordance with both the Public Health 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 Public Health Policy No. 1223, Safeguards for Protected Health information (PHI), G. Use of Electronic Systems, 2) E-mail and Attachment 1, Public Health Guidelines Governing the Use of E-Mail Involving Protected Health Information (PHI).

Internet based e-mail services accessed with County information technology must only be used for County purposes.

VII. USE OF THE INTERNET

Use of the Internet must be in accordance with Public Health and County Internet and privacy policies.

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

Users must not allow another User to access the Internet using their authorized account. Internet access is provided to the User at the discretion of each Public Health Facility.

VIII. RECORDABLE MOBILE DEVICES AND REMOVABLE MEDIA

Users must manage and control and ensure encryption, as per County standard, of all recordable mobile devices and removable media that contain PHI or other confidential information. These devices include PDA's, USB flash drives, cellular phones, cameras and camera phones, 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 Public Health Policy No. 1008, Workstation Use and Security: Access and Use of Mobile Devices.

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.

MALICIOUS SOFTWARE: The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms.

For a more complete definition of terms used in this policy and/or procedure, see the Public Health information Security Glossary Attachment I to Public Health Policy No. 1000 Public Health 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
6.110, Protection of Information on Portable Computing Devices

REFERENCE: Public Health Policies:
1201, Public Health Privacy and Security Compliance Program
1223, Safeguards for Protected Health Information (PHI)
1000, Public Health Information Technology and Security Policy
1008, Workstation Use and Security Policy

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 user 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 a 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. Confidentiality: I will not access 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.

5. 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.

6. 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.

7. 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

Initial _____

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.

8. 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.

9. Copyrighted materials: I will not copy any licensed software or documentation except as permitted by the license agreement.

10. 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, 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 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.

Initial _____

(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.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

Employee's Name	Employee's Signature	Date

Manager's Name	Manager's Signature	Date

Board of Supervisors Policy #6.101 Use of County Information Technology Resources Attachment
Revised: July 2004

ACKNOWLEDGMENT OF
PUBLIC HEALTH POLICY NO. 1016, ACCEPTABLE USE POLICY
FOR COUNTY INFORMATION TECHNOLOGY RESOURCES

I acknowledge that I have received and read Public Health Policy No. 1016, 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.

Name (print):	Employee No.:	Date:
Signature:	Job Title:	
Supervisor Name (print)	Supervisor Signature:	Date:

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