oneeapp
One Stop Access to Apply for Assistance

Attachment B: Los Angeles County

OEA User Account Application Additional Documents

September 2015

DEPARTMENT OF HEALTH SERVICES

Title:	Effective Date:
One-e-App (OEA) System User Agreement and Code of Ethics and Conduct	**JULY 2014**

This **System User Agreement** applies to all employees, contractors, subcontractors, vendors, volunteers and any other users of the County of Los Angeles (County) Department of Health Services (DHS) OEA System, whether permanent, temporary, part-time, or in any other status. Only authorized users are permitted to use the OEA System.

As an OEA System user, I understand and agree to the following:

1. I understand and agree that the OEA System is the property of the County and I will use the OEA System for only those specific County approved business purposes for which I am authorized. Personal, non-County business, and/or unauthorized use or access of the OEA System or OEA System information is forbidden, including personal use of the e-mail component and any other applications or software within the OEA System.

2. I understand and agree that I will have access to confidential DHS applicant and participant information for which there is an expectation of privacy. I shall protect, secure, and keep confidential all such OEA System information in compliance with all applicable federal, state, and local laws, rules, regulations, ordinances, guidelines, directives, policies, and procedures relating to confidentiality and information security, as well as County guidelines, directives, policies, and procedures relating to same. I agree to forward all requests for the disclosure or release of any OEA System information or data received by me to my immediate supervisor or manager.

3. I understand and agree that I will not subvert or bypass any security measures which have been implemented in order to control or restrict access to the OEA System nor will I attempt to use the OEA System in order to gain unauthorized access to any other computer systems or networks.

4. I understand and agree that I am responsible for maintaining the secrecy of my OEA System account and password, and I am fully responsible for all activities that occur with my account and password. I will not permit others to use my account or password in order to access the OEA System. I will immediately notify my immediate supervisor, manager, or Local Security Officer (LSO)* of any unauthorized use of my account or password, or any other breach of security, known or suspect. If I know or suspect that my account and password is known by someone other than myself, I must immediately change my password. *(The LSO is the person responsible for the administration of security policies at the local office level).

5. I understand and agree that I will not leave my workstation unattended while in active logon status to OEA. When I leave my workstation, I will either lock the workstation or logoff from the OEA System.

6. I understand and agree that it is illegal for me to knowingly access the OEA System to add, delete, alter, damage, destroy, copy or otherwise use the OEA System or data in order to defraud, deceive, extort, or control data for wrongful personal gain.

7. I understand and agree that I am not permitted to access, copy, or disclose any software, code, data, information, or related documentation from the OEA System to any individual or organization without specific written DHS management authorization.

8. I understand and agree that any or all uses or access of the OEA System, authorized or unauthorized, constitutes consent of its usage and data to be monitored, interrupted, recorded, read, copied or captured and disclosed in any manner for any lawful or authorized purpose, including in a disciplinary or civil action and criminal prosecution.

DEPARTMENT OF HEALTH SERVICES

One-e-App User Code of Ethics and Conduct

1. OEA Users are prohibited from providing application assistance to their immediate or extended family members of any relation, personal friends, or themselves. Family members and personal friends are to be referred to another impartial OEA User for their interview, screening, verification, collection, application submission, enrollment and changes in OEA. This is to ensure that an impartial and objective party is involved to remove any doubt of the information or documentation provided and to protect the integrity of the MHLA Program's application collection systems.

2. OEA Users may not participate in any activity or enterprise with clients or providers where income, profit or any other gain may be accrued that could reflect on the honor of efficiency of the MHLA Program service; or that may be contrary to the best interests of the MHLA Program.

3. OEA Users may not coach a client to give deceiving or otherwise false or misleading information in order for the client to become eligible for County/State/Federal programs. Doing so may constitute fraudulent activity.

4. OEA Users are prohibited from soliciting or accepting any gifts, gratuities, kickbacks, or anything of monetary value from clients, providers, contractors, or potential contractors. OEA Users are prohibited from attempting to secure payment or any other benefit for services rendered as an OEA User.

5. OEA Users should not use OEA services or the data to view or gather information about him or herself, co-workers or people with any personal relationship. People described above including family members and personal friends are to be referred to an impartial OEA User for their interview, screening, verification collection, application submission, enrollment and any changes in OEA. Refer to Section #1 above.

6. OEA Users may not disclose ANY information about applicants or their families, including but not limited to, their names, addresses, Social Security numbers, health status, or incomes to any other party. OEA Users must hold this information in the strictest of confidence and safeguard it from being revealed. Under NO circumstances should applicants receive solicitations or be placed on any mailing list unrelated to MHLA correspondence as a result of their application(s) or contact(s) with OEA Users.

7. OEA Users may never invite or influence any applicant or their dependents to separate from any form of health coverage or arrange for this to happen in order for the applicant to become eligible for the MHLA Program.

8. OEA Users may never coach or recommend one plan/provider over another.

9. Under no circumstances will OEA Users disclose their OEA username and passwords. OEA Users agree to notify the MHLA Program anytime they believe their username and password has been compromised or suspect that someone else has knowledge of their password.

<u>OEA Users Agree to:</u>

1. Assist applicants in properly completing the application and OEA process.
2. Ensure the confidentiality of all applications, records and any related information received in written, graphic, oral, or other tangible forms.
3. Answer questions pertaining to the MHLA application, program, and enrollment process.
4. Review and explain the documents that are required as part of the MHLA application.
5. Act in a courteous and professional manner at all times.
6. Abide by MHLA Program rules and enrollment procedures.

I understand that it is my responsibility to read and comply with the guidelines in this Agreement. I also understand that not following these guidelines could result in my losing access to OEA and/or user rights and that this information will be communicated to my supervisors and/or OEA Training Leads. I further understand that any violation of this Agreement as an authorized user may result in disciplinary action up to and including discharge, civil liability, and/or criminal prosecution as provided by federal and State of California laws and/or local ordinances. Non-employees, including contractors, may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

I recognize that my failure to abide by this Agreement and/or fulfill my security responsibilities could result in the abuse of OEA System information resources and data, and that the County may hold me responsible for such abuse. Wrongful access, inspection, use or disclosure of confidential OEA System information for personal gain, curiosity, or any non-business related reason is a crime under State and federal laws, including, but not limited to, the provisions of California Penal Code Section 502(c).

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.100	Information Technology and Security Policy	07/13/04

PURPOSE

To establish a Countywide Information Technology and Security program supported by countywide policies in order to assure appropriate and authorized access, usage and the integrity of County information and information technology assets.

REFERENCE

- Comprehensive Computer Data Access and Fraud Act, California Penal Code 502.
- Health Insurance Portability and Accountability Act (HIPAA) of 1996

POLICY

Information and the systems, networks, and software necessary for processing are essential County assets that must be appropriately protected against all forms of unauthorized access, use, disclosure, or modification. Security and controls for County information and associated information technology (I/T) assets which are owned, managed, operated, maintained, or in the custody or proprietorship of the County or non-County entities must be implemented to help ensure:

- Privacy and confidentiality
- Data integrity
- Availability
- Accountability
- Appropriate use

The County Technology and Security Policies will establish the minimum standard to which all departments must adhere. Departments may, at their discretion, enhance the minimum standard based on their unique requirements.

RESPONSIBILITIES

Departments, Commissions, Board and Offices

Department heads are responsible for ensuring appropriate I/T use and security within the Department. Departmental management is responsible for organizational adherence to countywide technology and security policies. They must ensure that all employees and other users of departmental information technology resources be made aware of those policies and that compliance is mandatory. They must also develop organizational procedures to support policy implementation.

The Department Head will ensure the designation of an individual to be responsible for coordinating appropriate use and information security within the Department.

Chief Information Office (CIO)

The Office of the CIO will ensure the development of countywide information technology policies that, in addition to security will specify the appropriate use of information technology (I/T) resources for internal and external activities, e-mail and other communications as well as Internet access and use. When approved, these policies will be published and made available to all users of County I/T resources to ensure their awareness and compliance.

Chief Information Security Officer (CISO)

The Chief Information Security Officer reports to the Chief Information Officer (CIO) and is responsible for the I/T Security Program for the County. Responsibilities include:

Developing and maintaining the information security strategy for the County

Chairing the Information Security Steering Committee (ISSC)

Providing information security related technical, regulatory, and policy leadership

Facilitating the implementation of County information security policies

Coordinating information security efforts across departmental lines

Leading information security training and education efforts

Directing the Countywide Computer Emergency Response Team (CCERT)

Departmental Information Technology Management/CIO will:

Manage information technology assets within the Department

Be responsible for any departmental information technology and security policy

Ensure that systems are implemented and configured to meet County information security standards

Ensure that systems are maintained at current critical security patch levels

Implement technology-based services that adhere to the intent and purpose of all information technology use and security policies, standards and guidelines

Individual designated as Security Coordinator or Departmental Information Security Officer (DISO) will:

Manage security of information technology assets within the Department

Assist in the development of departmental information technology security policy

Represent the Department at the Information Security Steering Committee (ISSC)

Coordinate the Departmental Computer Emergency Response Team (DCERT)

Employees and Other Authorized Users:

Employees and other department authorized users are responsible for acknowledging and adhering to County information technology use and security policies. They are responsible for protection of County information assets for which they are entrusted and using them for their intended purposes. Employees and authorized non-County users will be required to sign an "Acceptable Use Agreement" as a condition of being granted access to County I/T systems.

Information Security Steering Committee (ISSC)

The Information Security Steering Committee is established to be the coordinating body for all County information security-related activities and is composed of the Departmental Information Security Officers (DISO) or designated representative.

ISSC responsibilities include:

Assisting the CISO in developing, reviewing, and recommending information security policies

Identifying and recommending industry best practices for information security

Developing, reviewing and recommending countywide standards, procedures and guidelines

Coordinating inter-departmental communication and collaboration on security issues

Coordinating countywide I/T security education and awareness

Policy Exceptions

Requests for exceptions to this Board policy must be reviewed by the CIO and approved by the Board of Supervisors. Departments requesting exceptions should provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the department, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO will review such requests, confer with the requesting department and place the matter on the Board's agenda along with a recommendation for Board action.

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004	**Sunset Date: July 13, 2008**
Review Date: August 25, 2008	**Sunset Date: July 13, 2012**
Review Date: July 19, 2012	**Sunset Date: January 13, 2013**
Review Date: June 27, 2013	**Sunset Date: September 30, 2013**
Review Date: September 18, 2013	**Sunset Date: January 30, 2014**
Review Date: January 15, 2014	**Sunset Date: February 28, 2014**
Review Date: February 19, 2014	**Sunset Date: March 19, 2014**
Review Date: March 19, 2014	**Sunset Date: December 31, 2014**

PAGE < PAGE >

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.101	Use of County Information Technology Resources	07/13/04

PURPOSE

To establish policies under which users (County employees, contractors, sub-contractors, volunteers and other governmental and private agency staff) may make use of County Information Technology resources.

REFERENCE

July 10, 2004, Board Order 10 - Board of Supervisors Policy – Information Technology and Security Policy
Acceptable Use Agreement (Attached)

POLICY

County information technology resources are to be used for County business purposes.

County employees or other authorized user shall not share their unique (logon/system identifier) with any other person.

No user shall intentionally, or through negligence, damage, interfere with the operation of, or prevent authorized access to County information technology resources. It is every user's duty to use the County's resources responsibly, professionally, ethically, and lawfully.

The County has the right to administer any and all aspects of County information access and use including the right to monitor Internet, e-mail and data access.

Monitoring/investigating employee access to County I/T resources (i.e., e-mail, Internet or employee generated data files) must be approved by department management. If evidence of abuse is identified, notice must be provided to the Auditor-Controller's Office of County Investigations.

Users cannot expect the right to privacy in anything they create, store, send, or receive using County information technology resources.

All users of County information resources must sign an "Acceptable Use Agreement" prior to being granted access.

Definitions

County Information Technology Resources include but are not limited to the following:

- Computers and any electronic device which stores and/or processes County data (for example: desktops, laptops, midrange, mainframes, PDAs, County wired or wireless networks, digital cameras, copiers, IP phones, faxes, pagers, related peripherals, etc.)
- Storage media (diskettes, tapes, CDs, zip disk, DVD, etc.) on or off County premises.
- Network connections (wired and wireless) and infrastructure, including jacks, wiring, switches, patch panels, hubs, routers, etc.
- Data contained in County systems (databases, emails, documents repositories, web pages, etc.)
- County purchased, licensed, or developed software.

Access Control

Unauthorized access to any County information technology resources, including the computer system, network, software application programs, data files, and restricted work areas and County facilities is prohibited.

Access control mechanisms must be in place to protect against unauthorized use, disclosure, modification, or destruction of resources.

Access control mechanisms may include hardware, software, storage media, policy and procedures, and physical security.

Authentication

Access to every County system shall have an appropriate user authentication mechanism based on the sensitivity and level of risk associated with the data.

All County data systems containing data that requires restricted access shall require user authentication before access is granted.

County information technology resource users shall not allow others to access a system while it is logged on under their user sessions. The only exceptions allowed are when the software cannot be configured to enforce a log-in, or where the business needs of the Department require an alternate login practice for specified functions.

Representing yourself as someone else, real or fictional, or sending information anonymously is prohibited unless specifically authorized by department management.

County information technology resource users shall be responsible for the integrity of the authentication mechanism granted to them. For example, users shall not share their passwords, electronic cards, biometric logons, secure ID cards and/or other authentication mechanisms with others.

Fixed passwords, which are used for most access authorization, must be changed at least every 90 days.

Data Integrity

County information technology users are responsible for maintaining the integrity of County data. They shall not knowingly or through negligence cause County data to be modified or corrupted in any way that compromises its accuracy or prevents authorized access to it.

Accessing County Technology Resources Remotely

Access to County technology resources by an employee or non-County employee owned equipment must be approved by department management and/or be part of an approved contract. In all cases, the equipment being used for access must be compliant with County security software requirements.

Privacy

Information that is accessed using County information technology resources must be used for County authorized purposes and must not be disclosed to others.

Confidentiality

Unless expressly authorized by department management or policy; sending, disclosing, or otherwise disseminating confidential data, protected information, or other confidential information of the County is strictly prohibited. This includes information that is protected under HIPAA or any other privacy legislation.

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contractors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

Policy Exceptions

Requests for exceptions to this Board policy must be reviewed by the CIO and approved by the Board of Supervisors. Departments requesting exceptions should provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the department, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO will review such requests, confer with the requesting department and place the matter on the Board's agenda along with a recommendation for Board action.

(See Acceptable Use Agreement)

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004	**Sunset Date: July 13, 2008**
Review Date: August 25, 2008	**Sunset Date: July 13, 2012**
Review Date: July 19, 2012	**Sunset Date: January 13, 2013**
Review Date: June 27, 2013	**Sunset Date: September 30, 2013**
Review Date: September 18, 2013	**Sunset Date: January 30, 2014**
Review Date: January 15, 2014	**Sunset Date: February 28, 2014**
Review Date: February 19, 2014	**Sunset Date: March 19, 2014**
Review Date: March 19, 2014	**Sunset Date: December 31, 2014**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.102	Countywide Antivirus Security Policy	07/13/04

PURPOSE

To establish an antivirus security policy for the protection of all County information technology resources.

REFERENCE

July 10, 2004, Board Order 10 - Board of Supervisors Policy – Information Technology and Security Policy.

POLICY

Each department shall provide County-approved real-time virus protection for all County hardware/software environments to mitigate risk to County data, devices, and networks.

Antivirus software shall be configured to actively scan all files received by the computing device.

Each department shall ensure that antivirus software is updated when a new antivirus definition/software release is available and when hardware/software compatibility is confirmed.

Each department that maintains direct Internet access shall implement an antivirus system to scan Internet web pages, Internet e-mails, and File Transfer Protocol (FTP) downloads.

Each department must comply with the requirements of the CCERT policy in the notification of credible computer threat events.

Only authorized personnel shall make changes to the antivirus software configurations as required.

Any employee or authorized user who telecommutes or is granted remote access shall utilize equipment that contains current County-approved anti-virus software and shall adhere to County hardware/software protection standards and procedures that are defined for the County and the authorizing department.

County employees or authorized personnel are prohibited from intentionally introducing a virus or other malicious code into any device or the County's network or to deactivate or interfere with the operation of the antivirus software.

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.

Each department shall adhere to the standards and procedures set forth by this policy.

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contractors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

Policy Exceptions

Requests for exceptions to this Board policy must be reviewed by the CIO and approved by the Board of Supervisors. Departments requesting exceptions should provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the department, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO will review such requests, confer with the requesting department and place the matter on the Board's agenda along with a recommendation for Board action.

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004	**Sunset Date: July 13, 2008**
Review Date: August 21, 2008	**Sunset Date: July 13, 2012**
Review Date: July 19, 2012	**Sunset Date: January 13, 2013**
Review Date: June 27, 2013	**Sunset Date: September 30, 2013**
Review Date: September 18, 2013	**Sunset Date: January 30, 2014**
Review Date: January 15, 2014	**Sunset Date: February 28, 2014**
Review Date: February 19, 2014	**Sunset Date: March 19, 2014**
Review Date: March 19, 2014	**Sunset Date: December 31, 2014**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.109	Security Incident Reporting	05/08/07

PURPOSE

The intent of this policy is to ensure that County departments report information technology (IT) security incidents in a consistent manner to responsible County management to assist their decision and coordination process.

REFERENCE

Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information

May 8, 2007, Board Order No. 26

Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources

Board of Supervisors Policy No. 6.103 – Countywide Computer Security Threat Responses

Board of Supervisors Policy No. 6.110 – Protection of Information on Portable Computing Devices

POLICY

All information technology (IT) related security incidents (i.e., virus/worm attacks, actual or suspected loss or disclosure of personal and/or confidential information, etc.) must be reported to the applicable designated County offices in a timely manner to minimize the risk to the County, its employees and assets, and other persons/entities. The County department that receives a report of an incident must coordinate the information gathering and documenting process and collaborate with other affected departments to identify and implement a resolution or incident mitigation action (i.e., notification of unauthorized disclosure of personal and/or confidential information to the affected employee and/or

other person/entity, etc.)

In all cases, IT related security incidents must be reported by the Chief Information Office (CIO) to the Board of Supervisors (Board) delineating the scope of the incident, impact, actions being taken and any action taken to prevent a further occurrence. Board notification must occur as soon as the incident is known. Subsequent updates to the Board may occur until the incident is closed as determined by the Chief Information Security Officer (CISO).

Each County department must coordinate with one or both of the designated County offices (CIO and the Auditor-Controller), as applicable, when an IT related security incident occurs. For purposes of this coordination, the CISO has the responsibility for the CIO. The County HIPAA Privacy Officer (HPO) and the Office of County Investigations (OCI) have respective responsibilities for the Auditor-Controller.

Chief Information Security Officer (CISO)

All IT related security incidents that may result in the disruption of business continuity or actual or suspected loss or disclosure of personal and/or confidential information must be reported to the applicable. Departmental Information Security Officer (DISO) who will report to the CISO. Examples of these incidents include:

- Virus or worm outbreaks that infect at least ten (10) IT devices (i.e, desktop and laptop computers, personal digital assistants (PDA, etc.)
- Malicious attacks on IT networks
- Web page defacements
- Actual or suspected loss or disclosure of personal and/or confidential information
- Loss of County supplied portable computing devices (i.e., laptops, PDAs removable storage devices, etc.)

HIPAA Privacy Officer (HPO)

All IT related security incidents that may involve patient protected health information (PHI) must be reported by the affected County departments to the HPO. These incidents may be reported using an on-line form found at www.lacountyfraud.org. Examples of these incidents include:

- Compromise of patient information
- Actual or suspected loss or disclosure of patient information

Office of County Investigations (OCI)

All IT related security incidents that may involve non-compliance with any Acceptable Usage Agreement (Refer to Board of Supervisors Policy No. 6.101, Use of County Information Technology Resources) or the actual or suspected loss or disclosure of personal and/or confidential information must be reported to OCI. These incidents can be reported using an on-line form found at www.lacountyfraud.org. Examples of these incidents include:

- System breaches from internal or external sources
- Lost or stolen computers and data
- Inappropriate non-work related data which may include pornography, music, videos
- Actual or suspected loss or disclosure of personal and/or confidential information

Chief Information Office (CIO)

All IT related security incidents that affect multiple departments, create significant loss of productivity or result in the actual or suspected loss or disclosure of personal and/or confidential information shall be coordinated with the CIO/CISO. As soon as the pertinent facts are known, the incident will be reported by the CIO to the Board of Supervisors. The CISO shall be responsible for determining the facts related to the incident and updating the CIO and other affected persons/entities on a regular basis until the issue(s) are resolved as determined by the CIO and action(s) taken to prevent any further occurrence. A final report shall be developed by the CIO that describes the incident, cost of remediation and loss of productivity (where applicable), impact due to the actual or suspected los or disclosure of personal and/or confidential information, and final actions taken to mitigate and prevent future occurrences of similar events.

Actual or suspected loss or disclosure of personal and/or confidential information must result in a notification to the affected persons/entities via a formal letter from the applicable County department describing types of sensitive/confidential information lost and recommended actions to be taken by the persons/entities to mitigate the potential misuse of their information.

Definition Reference

As used in this policy, the terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contractors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007 **Sunset Review Date: May 8, 2011**
Issue Date: March 17, 2011 **Sunset Review Date: May 8, 2015**

WELFARE AND INSTITUTIONS CODE
SECTION 825-830.1

825. The order and findings of the superior court in each case under the provisions of this chapter shall be entered in a suitable book or other form of written record which shall be kept for that purpose and known as the "juvenile court record."

826. (a) After five years from the date on which the jurisdiction of the juvenile court over a minor is terminated, the probation officer may destroy all records and papers in the proceedings concerning the minor.

The juvenile court record, which includes all records and papers, any minute book entries, dockets and judgment dockets, shall be destroyed by order of the court as follows: when the person who is the subject of the record reaches the age of 28 years, if the person was alleged or adjudged to be a person described by Section 300, when the person who is the subject of the record reaches the age of 21 years, if the person was alleged or adjudged to be a person described by Section 601, or when the person reaches the age of 38 years if the person was alleged or adjudged to be a person described by Section 602, unless for good cause the court determines that the juvenile record shall be retained, or unless the juvenile court record is released to the person who is the subject of the record pursuant to this section. However, a juvenile court record which is not permitted to be sealed pursuant to subdivision (f) of Section 781 shall not be destroyed pursuant to this section.

Any person who is the subject of a juvenile court record may by written notice request the juvenile court to release the court record to his or her custody. Wherever possible, the written notice shall include the person's full name, the person's date of birth, and the juvenile court case number. Any juvenile court receiving the written notice shall release the court record to the person who is the subject of the record five years after the jurisdiction of the juvenile court over the person has terminated, if the person was alleged or adjudged to be a person described by Section 300, or when the person reaches the age of 21 years, if the person was alleged or adjudged to be a person described by Section 601, unless for good cause the court determines that the record shall be retained. Exhibits shall be destroyed as provided under Section 1417 of the Penal Code. For the purpose of this section "destroy" means destroy or dispose of for the purpose of destruction. The proceedings in any case in which the juvenile court record is destroyed or released to the person who is the subject of the record pursuant to this section shall be deemed never to have occurred, and the person may reply accordingly to any inquiry about the events in the case.

(b) If an individual whose juvenile court record has been destroyed or released under subdivision (a) discovers that any other

agency still retains a record, the individual may file a petition with the court requesting that the records be destroyed. The petition will include the name of the agency and the type of record to be destroyed. The court shall order that such records also be destroyed unless for good cause the court determines to the contrary. The court shall send a copy of the order to each agency and each agency shall destroy records in its custody as directed by the order, and shall advise the court of its compliance. The court shall then destroy the copy of the petition, the order, and the notice of compliance from each agency. Thereafter, the proceedings in such case shall be deemed never to have occurred.

(c) Juvenile court records in juvenile traffic matters, which include all records and papers, any minute book entries, dockets and judgment dockets, may be destroyed after five years from the date on which the jurisdiction of the juvenile court over a minor is terminated, or when the minor reaches the age of 21 years, if the person was alleged or adjudged to be a person described by Section 601. Prior to such destruction the original record may be microfilmed or photocopied. Every such reproduction shall be deemed and considered an original; and a transcript, exemplification or certified copy of any such reproduction shall be deemed and considered a transcript, exemplification or certified copy, as the case may be, of the original.

826.5. (a) Notwithstanding the provisions of Section 826, at any time before a person reaches the age when his or her records are required to be destroyed, the judge or clerk of the juvenile court or the probation officer may destroy all records and papers, the juvenile court record, any minute book entries, dockets, and judgment dockets in the proceedings concerning the person as a minor if the records and papers, juvenile court record, any minute book entries, dockets, and judgment dockets are microfilmed or photocopied prior to destruction. Exhibits shall be destroyed as provided under Sections 1418, 1418.5, and 1419 of the Penal Code.

(b) Every reproduction shall be deemed and considered an original. A transcript, exemplification, or certified copy of any reproduction shall be deemed and considered a transcript, exemplification, or certified copy, as the case may be, of the original.

826.6. (a) Any minor who is the subject of a petition that has been filed in juvenile court to adjudge the minor a dependent child or a ward of the court shall be given written notice by the clerk of the court upon disposition of the petition or the termination of jurisdiction of the juvenile court of all of the following:

(1) The statutory right of any person who has been the subject of juvenile court proceedings to petition for sealing of the case records.

(2) The statutory provisions regarding the destruction of juvenile court records and records of juvenile court proceedings retained by state or local agencies.

(3) The statutory right of any person who has been the subject of juvenile court proceedings to have his or her juvenile court record released to him or her in lieu of its destruction.

(b) In any juvenile case where a local welfare department, probation department, or district attorney is responsible for notifying the minor of the dismissal, release, or termination of the case, the agency shall provide written notice to the minor of the information specified in subdivision (a) upon the dismissal, release, or termination of the case.

(c) A written form providing the information described in this section shall be prepared by the clerk of the court and shall be made available to juvenile court clerks, probation departments, welfare departments, and district attorneys.

826.7. Juvenile case files that pertain to a child who died as the result of abuse or neglect shall be released by the custodian of records of the county welfare department or agency to the public pursuant to Section 10850.4 or an order issued pursuant to paragraph (2) of subdivision (a) of Section 827.

827. (a) (1) Except as provided in Section 828, a case file may be inspected only by the following:

(A) Court personnel.

(B) The district attorney, a city attorney, or city prosecutor authorized to prosecute criminal or juvenile cases under state law.

(C) The minor who is the subject of the proceeding.

(D) The minor's parents or guardian.

(E) The attorneys for the parties, judges, referees, other hearing officers, probation officers, and law enforcement officers who are actively participating in criminal or juvenile proceedings involving the minor.

(F) The county counsel, city attorney, or any other attorney representing the petitioning agency in a dependency action.

(G) The superintendent or designee of the school district where the minor is enrolled or attending school.

(H) Members of the child protective agencies as defined in Section 11165.9 of the Penal Code.

(I) The State Department of Social Services, to carry out its duties pursuant to Division 9 (commencing with Section 10000), and Part 5 (commencing with Section 7900) of Division 12, of the Family Code to oversee and monitor county child welfare agencies, children in foster care or receiving foster care assistance, and out-of-state placements, Section 10850.4, and paragraph (2).

(J) Authorized legal staff or special investigators who are peace officers who are employed by, or who are authorized representatives of, the State Department of Social Services, as necessary to the performance of their duties to inspect, license, and investigate community care facilities, and to ensure that the standards of care and services provided in those facilities are adequate and appropriate and to ascertain compliance with the rules and regulations to which the facilities are subject. The confidential information shall remain confidential except for purposes of inspection, licensing, or investigation pursuant to Chapter 3 (commencing with Section 1500) and Chapter 3.4 (commencing with Section 1596.70) of Division 2 of the Health and Safety Code, or a criminal, civil, or administrative proceeding in relation thereto.

The confidential information may be used by the State Department of Social Services in a criminal, civil, or administrative proceeding. The confidential information shall be available only to the judge or hearing officer and to the parties to the case. Names that are confidential shall be listed in attachments separate to the general pleadings. The confidential information shall be sealed after the conclusion of the criminal, civil, or administrative hearings, and may not subsequently be released except in accordance with this subdivision. If the confidential information does not result in a criminal, civil, or administrative proceeding, it shall be sealed after the State Department of Social Services decides that no further action will be taken in the matter of suspected licensing violations. Except as otherwise provided in this subdivision, confidential information in the possession of the State Department of Social Services may not contain the name of the minor.

(K) Members of children's multidisciplinary teams, persons, or agencies providing treatment or supervision of the minor.

(L) A judge, commissioner, or other hearing officer assigned to a family law case with issues concerning custody or visitation, or both, involving the minor, and the following persons, if actively participating in the family law case: a family court mediator assigned to a case involving the minor pursuant to Article 1 (commencing with Section 3160) of Chapter 11 of Part 2 of Division 8 of the Family Code, a court-appointed evaluator or a person conducting a court-connected child custody evaluation, investigation, or assessment pursuant to Section 3111 or 3118 of the Family Code, and counsel appointed for the minor in the family law case pursuant to Section 3150 of the Family Code. Prior to allowing counsel appointed for the minor in the family law case to inspect the file, the court clerk may require counsel to provide a certified copy of the court order appointing him or her as the minor's counsel.

(M) A court-appointed investigator who is actively participating in a guardianship case involving a minor pursuant to Part 2 (commencing with Section 1500) of Division 4 of the Probate Code and acting within the scope of his or her duties in that case.

(N) A local child support agency for the purpose of establishing paternity and establishing and enforcing child support orders.

(O) Juvenile justice commissions as established under Section 225. The confidentiality provisions of Section 10850 shall apply to a juvenile justice commission and its members.

(P) Any other person who may be designated by court order of the judge of the juvenile court upon filing a petition.

(2) (A) Notwithstanding any other law and subject to subparagraph (A) of paragraph (3), juvenile case files, except those relating to matters within the jurisdiction of the court pursuant to Section 601 or 602, that pertain to a deceased child who was within the jurisdiction of the juvenile court pursuant to Section 300, shall be released to the public pursuant to an order by the juvenile court after a petition has been filed and interested parties have been afforded an opportunity to file an objection. Any information relating to another child or which could identify another child, except for information about the deceased, shall be redacted from the juvenile case file prior to release, unless a specific order is made by the juvenile court to the contrary. Except as provided in this paragraph, the presiding judge of the juvenile court may issue an order prohibiting or limiting access to the juvenile case file, or any portion thereof, of a deceased child only upon a showing by a

preponderance of evidence that release of the juvenile case file or any portion thereof is detrimental to the safety, protection, or physical or emotional well-being of another child who is directly or indirectly connected to the juvenile case that is the subject of the petition.

(B) This paragraph represents a presumption in favor of the release of documents when a child is deceased unless the statutory reasons for confidentiality are shown to exist.

(C) If a child whose records are sought has died, and documents are sought pursuant to this paragraph, no weighing or balancing of the interests of those other than a child is permitted.

(D) A petition filed under this paragraph shall be served on interested parties by the petitioner, if the petitioner is in possession of their identity and address, and on the custodian of records. Upon receiving a petition, the custodian of records shall serve a copy of the request upon all interested parties that have not been served by the petitioner or on the interested parties served by the petitioner if the custodian of records possesses information, such as a more recent address, indicating that the service by the petitioner may have been ineffective.

(E) The custodian of records shall serve the petition within 10 calendar days of receipt. If any interested party, including the custodian of records, objects to the petition, the party shall file and serve the objection on the petitioning party no later than 15 calendar days of service of the petition.

(F) The petitioning party shall have 10 calendar days to file any reply. The juvenile court shall set the matter for hearing no more than 60 calendar days from the date the petition is served on the custodian of records. The court shall render its decision within 30 days of the hearing. The matter shall be decided solely upon the basis of the petition and supporting exhibits and declarations, if any, the objection and any supporting exhibits or declarations, if any, and the reply and any supporting declarations or exhibits thereto, and argument at hearing. The court may solely upon its own motion order the appearance of witnesses. If no objection is filed to the petition, the court shall review the petition and issue its decision within 10 calendar days of the final day for filing the objection. Any order of the court shall be immediately reviewable by petition to the appellate court for the issuance of an extraordinary writ.

(3) Access to juvenile case files pertaining to matters within the jurisdiction of the juvenile court pursuant to Section 300 shall be limited as follows:

(A) If a juvenile case file, or any portion thereof, is privileged or confidential pursuant to any other state law or federal law or regulation, the requirements of that state law or federal law or regulation prohibiting or limiting release of the juvenile case file or any portions thereof shall prevail. Unless a person is listed in subparagraphs (A) to (O), inclusive, of paragraph (1) and is entitled to access under the other state law or federal law or regulation without a court order, all those seeking access, pursuant to other authorization, to portions of, or information relating to the contents of, juvenile case files protected under another state law or federal law or regulation, shall petition the juvenile court. The juvenile court may only release the portion of, or information relating to the contents of, juvenile case files protected by another state law or federal law or regulation if disclosure is not

detrimental to the safety, protection, or physical or emotional well-being of a child who is directly or indirectly connected to the juvenile case that is the subject of the petition. This paragraph shall not be construed to limit the ability of the juvenile court to carry out its duties in conducting juvenile court proceedings.

(B) Prior to the release of the juvenile case file or any portion thereof, the court shall afford due process, including a notice of and an opportunity to file an objection to the release of the record or report to all interested parties.

(4) A juvenile case file, any portion thereof, and information relating to the content of the juvenile case file, may not be disseminated by the receiving agencies to any persons or agencies, other than those persons or agencies authorized to receive documents pursuant to this section. Further, a juvenile case file, any portion thereof, and information relating to the content of the juvenile case file, may not be made as an attachment to any other documents without the prior approval of the presiding judge of the juvenile court, unless it is used in connection with and in the course of a criminal investigation or a proceeding brought to declare a person a dependent child or ward of the juvenile court.

(5) Individuals listed in subparagraphs (A), (B), (C), (D), (E), (F), (H), and (I) of paragraph (1) may also receive copies of the case file. In these circumstances, the requirements of paragraph (4) shall continue to apply to the information received.

(b) (1) While the Legislature reaffirms its belief that juvenile court records, in general, should be confidential, it is the intent of the Legislature in enacting this subdivision to provide for a limited exception to juvenile court record confidentiality to promote more effective communication among juvenile courts, family courts, law enforcement agencies, and schools to ensure the rehabilitation of juvenile criminal offenders as well as to lessen the potential for drug use, violence, other forms of delinquency, and child abuse.

(2) Notwithstanding subdivision (a), written notice that a minor enrolled in a public school, kindergarten to grade 12, inclusive, has been found by a court of competent jurisdiction to have committed any felony or any misdemeanor involving curfew, gambling, alcohol, drugs, tobacco products, carrying of weapons, a sex offense listed in Section 290 of the Penal Code, assault or battery, larceny, vandalism, or graffiti shall be provided by the court, within seven days, to the superintendent of the school district of attendance. Written notice shall include only the offense found to have been committed by the minor and the disposition of the minor's case. This notice shall be expeditiously transmitted by the district superintendent to the principal at the school of attendance. The principal shall expeditiously disseminate the information to those counselors directly supervising or reporting on the behavior or progress of the minor. In addition, the principal shall disseminate the information to any teacher or administrator directly supervising or reporting on the behavior or progress of the minor whom the principal believes needs the information to work with the pupil in an appropriate fashion, to avoid being needlessly vulnerable or to protect other persons from needless vulnerability.

Any information received by a teacher, counselor, or administrator under this subdivision shall be received in confidence for the limited purpose of rehabilitating the minor and protecting students and staff, and shall not be further disseminated by the teacher, counselor, or administrator, except insofar as communication with the

juvenile, his or her parents or guardians, law enforcement personnel, and the juvenile's probation officer is necessary to effectuate the juvenile's rehabilitation or to protect students and staff.

An intentional violation of the confidentiality provisions of this paragraph is a misdemeanor punishable by a fine not to exceed five hundred dollars ($500).

(3) If a minor is removed from public school as a result of the court's finding described in subdivision (b), the superintendent shall maintain the information in a confidential file and shall defer transmittal of the information received from the court until the minor is returned to public school. If the minor is returned to a school district other than the one from which the minor came, the parole or probation officer having jurisdiction over the minor shall so notify the superintendent of the last district of attendance, who shall transmit the notice received from the court to the superintendent of the new district of attendance.

(c) Each probation report filed with the court concerning a minor whose record is subject to dissemination pursuant to subdivision (b) shall include on the face sheet the school at which the minor is currently enrolled. The county superintendent shall provide the court with a listing of all of the schools within each school district, within the county, along with the name and mailing address of each district superintendent.

(d) Each notice sent by the court pursuant to subdivision (b) shall be stamped with the instruction: "Unlawful Dissemination Of This Information Is A Misdemeanor." Any information received from the court shall be kept in a separate confidential file at the school of attendance and shall be transferred to the minor's subsequent schools of attendance and maintained until the minor graduates from high school, is released from juvenile court jurisdiction, or reaches the age of 18 years, whichever occurs first. After that time the confidential record shall be destroyed. At any time after the date by which a record required to be destroyed by this section should have been destroyed, the minor or his or her parent or guardian shall have the right to make a written request to the principal of the school that the minor's school records be reviewed to ensure that the record has been destroyed. Upon completion of any requested review and no later than 30 days after the request for the review was received, the principal or his or her designee shall respond in writing to the written request and either shall confirm that the record has been destroyed or, if the record has not been destroyed, shall explain why destruction has not yet occurred.

Except as provided in paragraph (2) of subdivision (b), no liability shall attach to any person who transmits or fails to transmit any notice or information required under subdivision (b).

(e) For purposes of this section, a "juvenile case file" means a petition filed in any juvenile court proceeding, reports of the probation officer, and all other documents filed in that case or made available to the probation officer in making his or her report, or to the judge, referee, or other hearing officer, and thereafter retained by the probation officer, judge, referee, or other hearing officer.

827.1. (a) Notwithstanding any other provision of law, a city,

county, or city and county may establish a computerized data base system within that city, county, or city and county that permits the probation department, law enforcement agencies, and school districts to access probation department, law enforcement, school district, and juvenile court information and records which are nonprivileged and where release is authorized under state or federal law or regulation, regarding minors under the jurisdiction of the juvenile court pursuant to Section 602 or for whom a program of supervision has been undertaken where a petition could otherwise be filed pursuant to Section 602.

(b) Each city, county, or city and county permitting computer access to these agencies shall develop security procedures by which unauthorized personnel cannot access data contained in the system as well as procedures or devices to secure data from unauthorized access or disclosure. The right of access granted shall not include the right to add, delete, or alter data without the written permission of the agency holding the data.

827.10. (a) Notwithstanding Section 827, the child welfare agency is authorized to permit its files and records relating to a minor, who is the subject of either a family law or a probate guardianship case involving custody or visitation issues, or both, to be inspected by, and to provide copies to, the following persons, if these persons are actively participating in the family law or probate case:

(1) The judge, commissioner, or other hearing officer assigned to the family law or probate case.

(2) The parent or guardian of the minor.

(3) An attorney for a party to the family law or probate case.

(4) A family court mediator assigned to a case involving the minor pursuant to Article 1 (commencing with Section 3160) of Chapter 11 of Part 2 of Division 8 of the Family Code.

(5) A court-appointed investigator, evaluator, or a person conducting a court-connected child custody evaluation, investigation, or assessment pursuant to Section 3111 or 3118 of the Family Code or Part 2 (commencing with Section 1500) of Division 4 of the Probate Code.

(6) Counsel appointed for the minor in the family law case pursuant to Section 3150 of the Family Code. Prior to allowing counsel appointed for the minor in the family law case to inspect the file, the court clerk may require counsel to provide a certified copy of the court order appointing him or her as the counsel for the minor.

(b) If the child welfare agency files or records, or any portions thereof, are privileged or confidential pursuant to any other state law, except Section 827, or federal law or regulation, the requirements of that state law or federal law or regulation prohibiting or limiting release of the child welfare agency files or records, or any portions thereof, shall prevail.

(c) A social worker may testify in any family or probate proceeding with regard to any information that may be disclosed under this section.

(d) Any records or information obtained pursuant to this section, including the testimony of a social worker, shall be maintained solely in the confidential portion of the family law or probate file.

827.2. (a) Notwithstanding Section 827 or any other provision of law, written notice that a minor has been found by a court of competent jurisdiction to have committed any felony pursuant to Section 602 shall be provided by the court within seven days to the sheriff of the county in which the offense was committed and to the sheriff of the county in which the minor resides. Written notice shall include only that information regarding the felony offense found to have been committed by the minor and the disposition of the minor's case. If at any time thereafter the court modifies the disposition of the minor's case, it shall also notify the sheriff as provided above. The sheriff may disseminate the information to other law enforcement personnel upon request, provided that he or she reasonably believes that the release of this information is generally relevant to the prevention or control of juvenile crime.

(b) Any information received pursuant to this section shall be received in confidence for the limited law enforcement purpose for which it was provided and shall not be further disseminated except as provided in this section. An intentional violation of the confidentiality provisions of this section is a misdemeanor punishable by a fine not to exceed five hundred dollars ($500).

(c) Notwithstanding subdivision (a) or (b), a law enforcement agency may disclose to the public or to any interested person the information received pursuant to subdivision (a) regarding a minor 14 years of age or older who was found by the court to have committed any felony enumerated in subdivision (b) of Section 707. The law enforcement agency shall not release this information if the court for good cause, with a written statement of reasons, so orders.

827.5. Notwithstanding any other provision of law except Sections 389 and 781 of this code and Section 1203.45 of the Penal Code, a law enforcement agency may disclose the name of any minor 14 years of age or older taken into custody for the commission of any serious felony, as defined in subdivision (c) of Section 1192.7 of the Penal Code, and the offenses allegedly committed, upon the request of interested persons, following the minor's arrest for that offense.

827.6. A law enforcement agency may release the name, description, and the alleged offense of any minor alleged to have committed a violent offense, as defined in subdivision (c) of Section 667.5 of the Penal Code, and against whom an arrest warrant is outstanding, if the release of this information would assist in the apprehension of the minor or the protection of public safety. Neither the agency nor the city, county, or city and county in which the agency is located shall be liable for civil damages resulting from release of this information.

827.7. (a) Notwithstanding Section 827 or any other provision of law, written notice that a minor has been found by a court of competent jurisdiction to have committed any felony pursuant to

Section 602 shall be provided by the court within seven days to the sheriff of the county in which the offense was committed and to the sheriff of the county in which the minor resides. Written notice shall include only that information regarding the felony offense found to have been committed by the minor and the disposition of the minor's case. If at any time thereafter the court modifies the disposition of the minor's case, it shall also notify the sheriff as provided above. The sheriff may disseminate the information to other law enforcement personnel upon request, provided that he or she reasonably believes that the release of this information is generally relevant to the prevention or control of juvenile crime.

Any information received pursuant to this section shall be received in confidence for the limited law enforcement purpose for which it was provided and shall not be further disseminated except as provided in this section. An intentional violation of the confidentiality provisions of this section is a misdemeanor punishable by a fine not to exceed five hundred dollars ($500).

(b) In the written notice provided pursuant to this section, a court may authorize a sheriff who receives information under this section to disclose this information where the release of the information is imperative for the protection of the public and the offense is a violent felony, as defined in subdivision (c) of Section 667.5 of the Penal Code.

827.9. (a) It is the intent of the Legislature to reaffirm its belief that records or information gathered by law enforcement agencies relating to the taking of a minor into custody, temporary custody, or detention (juvenile police records) should be confidential. Confidentiality is necessary to protect those persons from being denied various opportunities, to further the rehabilitative efforts of the juvenile justice system, and to prevent the lifelong stigma that results from having a juvenile police record. Although these records generally should remain confidential, the Legislature recognizes that certain circumstances require the release of juvenile police records to specified persons and entities. The purpose of this section is to clarify the persons and entities entitled to receive a complete copy of a juvenile police record, to specify the persons or entities entitled to receive copies of juvenile police records with certain identifying information about other minors removed from the record, and to provide procedures for others to request a copy of a juvenile police record. This section does not govern the release of police records involving a minor who is the witness to or victim of a crime who is protected by other laws including, but not limited to, Section 841.5 of the Penal Code, Section 11167 et seq. of the Penal Code, and Section 6254 of the Government Code.

(b) Except as provided in Sections 389 and 781 of this code or Section 1203.45 of the Penal Code, a law enforcement agency shall release, upon request, a complete copy of a juvenile police record, as defined in subdivision (m), without notice or consent from the person who is the subject of the juvenile police record to the following persons or entities:

(1) Other law enforcement agencies including the office of the Attorney General of California, any district attorney, the Department of Corrections and Rehabilitation, including the Division of

Juvenile Justice, and any peace officer as specified in subdivision (a) of Section 830.1 of the Penal Code.

(2) School district police.

(3) Child protective agencies as defined in Section 11165.9 of the Penal Code.

(4) The attorney representing the juvenile who is the subject of the juvenile police record in a criminal or juvenile proceeding.

(5) The Department of Motor Vehicles.

(c) Except as provided in Sections 389 and 781 of this code or Section 1203.45 of the Penal Code, law enforcement agencies shall release, upon request, a copy of a juvenile police record to the following persons and entities only if identifying information pertaining to any other juvenile, within the meaning of subdivision (n), has been removed from the record:

(1) The person who is the subject of the juvenile police record.

(2) The parents or guardian of a minor who is the subject of the juvenile police record.

(3) An attorney for a parent or guardian of a minor who is the subject of the juvenile police record.

(d) (1) (A) If a person or entity listed in subdivision (c) seeks to obtain a complete copy of a juvenile police record that contains identifying information concerning the taking into custody or detention of any other juvenile, within the meaning of subdivision (n), who is not a dependent child or a ward of the juvenile court, that person or entity shall submit a completed Petition to Obtain Report of Law Enforcement Agency, as developed pursuant to subdivision (i), to the appropriate law enforcement agency. The law enforcement agency shall send a notice to the following persons that a Petition to Obtain Report of Law Enforcement Agency has been submitted to the agency:

(i) The juvenile about whom information is sought.

(ii) The parents or guardian of any minor described in subparagraph (i). The law enforcement agency shall make reasonable efforts to obtain the address of the parents or guardian.

(B) For purposes of responding to a request submitted pursuant to this subdivision, a law enforcement agency may check the Juvenile Automated Index or may contact the juvenile court to determine whether a person is a dependent child or a ward of the juvenile court and whether parental rights have been terminated or the juvenile has been emancipated.

(C) The notice sent pursuant to this subdivision shall include the following information:

(i) The identity of the person or entity requesting a copy of the juvenile police record.

(ii) A copy of the completed Petition to Obtain Report of Law Enforcement Agency.

(iii) The time period for submitting an objection to the law enforcement agency, which shall be 20 days if notice is provided by mail or confirmed fax, or 15 days if notice is provided by personal service.

(iv) The means to submit an objection.

A law enforcement agency shall issue notice pursuant to this section within 20 days of the request. If no objections are filed, the law enforcement agency shall release the juvenile police record within 15 days of the expiration of the objection period.

(D) If any objections to the disclosure of the other juvenile's information are submitted to the law enforcement agency, the law

enforcement agency shall send the completed Petition to Obtain Report of Law Enforcement Agency, the objections, and a copy of the requested juvenile police record to the presiding judge of the juvenile court or, in counties with no presiding judge of the juvenile court, the judge of the juvenile court or his or her designee, to obtain authorization from the court to release a complete copy of the juvenile police record.

(2) If a person or entity listed in subdivision (c) seeks to obtain a complete copy of a juvenile police record that contains identifying information concerning the taking into custody or detention of any other juvenile, within the meaning of subdivision (n), who is a dependent child or a ward of the juvenile court, that person or entity shall submit a Petition to Obtain Report of Law Enforcement Agency, as developed pursuant to subdivision (i), to the appropriate law enforcement agency. The law enforcement agency shall send that Petition to Obtain Report of Law Enforcement Agency and a completed petition for authorization to release the information to that person or entity along with a complete copy of the requested juvenile police record to the presiding judge of the juvenile court, or, in counties with no presiding judge of the juvenile court, the judge of the juvenile court or his or her designees. The juvenile court shall provide notice of the petition for authorization to the following persons:

(A) If the person who would be identified if the information is released is a minor who is a dependent child of the juvenile court, notice of the petition shall be provided to the following persons:

(i) The minor.

(ii) The attorney of record for the minor.

(iii) The parents or guardian of the minor, unless parental rights have been terminated.

(iv) The child protective agency responsible for the minor.

(v) The attorney representing the child protective agency responsible for the minor.

(B) If the person who would be identified if the information is released is a ward of the juvenile court, notice of the petition shall be provided to the following:

(i) The ward.

(ii) The attorney of record for the ward.

(iii) The parents or guardian of the ward if the ward is under 18 years of age, unless parental rights have been terminated.

(iv) The district attorney.

(v) The probation department.

(e) Except as otherwise provided in this section or in Sections 389 and 781 of this code or Section 1203.45 of the Penal Code, law enforcement agencies shall release copies of juvenile police records to any other person designated by court order upon the filing of a Petition to Obtain Report of Law Enforcement Agency with the juvenile court. The petition shall be filed with the presiding judge of the juvenile court, or, in counties with no presiding judge of the juvenile court, the judge of the juvenile court or his or her designee, in the county where the juvenile police record is maintained.

(f) (1) After considering the petition and any objections submitted to the juvenile court pursuant to paragraph (1) or (2) of subdivision (d), the court shall determine whether the law enforcement agency may release a complete copy of the juvenile police record to the person or entity that submitted the request.

(2) In determining whether to authorize the release of a juvenile police record, the court shall balance the interests of the juvenile who is the subject of the record, the petitioner, and the public. The juvenile court may issue orders prohibiting or limiting the release of information contained in the juvenile police record. The court may also deny the existence of a juvenile police record where the record is properly sealed or the juvenile who is the subject of the record has properly denied its existence.

(3) Prior to authorizing the release of any juvenile police record, the juvenile court shall ensure that notice and an opportunity to file an objection to the release of the record has been provided to the juvenile who is the subject of the record or who would be identified if the information is released, that person's parents or guardian if he or she is under 18 years of age, and any additional person or entity described in subdivision (d), as applicable. The period for filing an objection shall be 20 days from the date notice is given if notice is provided by mail or confirmed fax and 15 days from the date notice is given if notice is provided by personal service. If review of the petition is urgent, the petitioner may file a motion with the presiding judge of the juvenile court showing good cause why the objection period should be shortened. The court shall issue a ruling on the completed petition within 15 days of the expiration of the objection period.

(g) Any out-of-state entity comparable to the California entities listed in paragraphs (1) to (5), inclusive, of subdivision (b) shall file a petition with the presiding judge of the juvenile court in the county where the juvenile police record is maintained in order to receive a copy of a juvenile police record. A petition from that entity may be granted on an ex parte basis.

(h) Nothing in this section shall require the release of confidential victim or witness information protected by other laws including, but not limited to, Section 841.5 of the Penal Code, Section 11167 et seq. of the Penal Code, and Section 6254 of the Government Code.

(i) The Judicial Council, in consultation with the California Law Enforcement Association of Record Supervisors (CLEARS), shall develop forms for distribution by law enforcement agencies to the public to implement this section. Those forms shall include, but are not limited to, the Petition to Obtain Report of Law Enforcement Agency. The material for the public shall include information about the persons who are entitled to a copy of the juvenile police record and the specific procedures for requesting a copy of the record if a petition is necessary. The Judicial Council shall provide law enforcement agencies with suggested forms for compliance with the notice provisions set forth in subdivision (d).

(j) Any information received pursuant to subdivisions (a) to (e), inclusive, and (g) of this section shall be received in confidence for the limited purpose for which it was provided and shall not be further disseminated. An intentional violation of the confidentiality provisions of this section is a misdemeanor, punishable by a fine not to exceed five hundred dollars ($500).

(k) A court shall consider any information relating to the taking of a minor into custody, if the information is not contained in a record which has been sealed, for purposes of determining whether an adjudication of the commission of a crime as a minor warrants a finding that there are circumstances in aggravation pursuant to Section 1170 of the Penal Code or to deny probation.

(l) When a law enforcement agency has been notified pursuant to Section 1155 that a minor has escaped from a secure detention facility, the law enforcement agency shall release the name of, and any descriptive information about, the minor to a person who specifically requests this information. The law enforcement agency may release the information on the minor without a request to do so if it finds that release of the information would be necessary to assist in recapturing the minor or that it would be necessary to protect the public from substantial physical harm.

(m) For purposes of this section, a "juvenile police record" refers to records or information relating to the taking of a minor into custody, temporary custody, or detention.

(n) For purposes of this section, with respect to a juvenile police record, "any other juvenile" refers to additional minors who were taken into custody or temporary custody, or detained and who also could be considered a subject of the juvenile police record.

(o) An evaluation of the efficacy of the procedures for the release of police records containing information about minors as described in this section shall be conducted by the juvenile court and law enforcement in Los Angeles County and the results of that evaluation shall be reported to the Legislature on or before December 31, 2006.

(p) This section shall only apply to Los Angeles County.

828. (a) Except as provided in Sections 389, 781, and 827.9 of this code or Section 1203.45 of the Penal Code, any information gathered by a law enforcement agency, including the Department of Justice, relating to the taking of a minor into custody may be disclosed to another law enforcement agency, including a school district police or security department, or to any person or agency which has a legitimate need for the information for purposes of official disposition of a case. When the disposition of a taking into custody is available, it shall be included with any information disclosed.

A court shall consider any information relating to the taking of a minor into custody, if the information is not contained in a record which has been sealed, for purposes of determining whether adjudications of commission of crimes as a juvenile warrant a finding that there are circumstances in aggravation pursuant to Section 1170 of the Penal Code or to deny probation.

(b) When a law enforcement agency has been notified pursuant to Section 1155 that a minor has escaped from a secure detention facility, the law enforcement agency shall release the name of, and any descriptive information about, the minor to a person who specifically requests this information. The law enforcement agency may release the information on the minor without a request to do so if it finds that release of the information would be necessary to assist in recapturing the minor or that it would be necessary to protect the public from substantial physical harm.

828.1. (a) While the Legislature reaffirms its belief that juvenile criminal records, in general, should be confidential, it is the intent of the Legislature in enacting this section to provide for a limited exception to that confidentiality in cases involving serious

acts of violence. Further, it is the intent of the Legislature that even in these selected cases the dissemination of juvenile criminal records be as limited as possible, consistent with the need to work with a student in an appropriate fashion, and the need to protect potentially vulnerable school staff and other students over whom the school staff exercises direct supervision and responsibility.

(b) Notwithstanding subdivision (a) of Section 828, a school district police or security department may provide written notice to the superintendent of the school district that a minor enrolled in a public school maintained by that school district, in kindergarten or any of grades 1 to 12, inclusive, has been found by a court of competent jurisdiction to have illegally used, sold, or possessed a controlled substance as defined in Section 11007 of the Health and Safety Code or to have committed any crime listed in paragraphs (1) to (15), inclusive, or paragraphs (17) to (19), inclusive, or paragraphs (25) to (28), inclusive, of subdivision (b) of, or in paragraph (2) of subdivision (d) of, or subdivision (e) of, Section 707. The information may be expeditiously transmitted to any teacher, counselor, or administrator with direct supervisorial or disciplinary responsibility over the minor, who the superintendent or his or her designee, after consultation with the principal at the school of attendance, believes needs this information to work with the student in an appropriate fashion, to avoid being needlessly vulnerable or to protect other persons from needless vulnerability.

(c) Any information received by a teacher, counselor, or administrator pursuant to this section shall be received in confidence for the limited purpose for which it was provided and shall not be further disseminated by the teacher, counselor, or administrator. An intentional violation of the confidentiality provisions of this section is a misdemeanor, punishable by a fine not to exceed five hundred dollars ($500).

828.3. Notwithstanding any other provision of law, information relating to the taking of a minor into custody on the basis that he or she has committed a crime against the property, students, or personnel of a school district or a finding by the juvenile court that the minor has committed such a crime may be exchanged between law enforcement personnel, the school district superintendent, and the principal of a public school in which the minor is enrolled as a student if the offense was against the property, students, or personnel of that school.

829. Notwithstanding any other provision of law, the Board of Prison Terms, in order to evaluate the suitability for release of a person before the board, shall be entitled to review juvenile court records which have not been sealed, concerning the person before the board, if those records relate to a case in which the person was found to have committed an offense which brought the person within the jurisdiction of the juvenile court pursuant to Section 602.

830. (a) Notwithstanding any other provision of law, members of a multidisciplinary personnel team engaged in the prevention,

identification, management, or treatment of child abuse or neglect may disclose and exchange information and writings to and with one another relating to any incidents of child abuse that may also be a part of a juvenile court record or otherwise designated as confidential under state law if the member of the team having that information or writing reasonably believes it is generally relevant to the prevention, identification, management, or treatment of child abuse, or the provision of child welfare services. All discussions relative to the disclosure or exchange of any such information or writings during team meetings are confidential unless disclosure is required by law. Notwithstanding any other provision of law, testimony concerning any such discussion is not admissible in any criminal, civil, or juvenile court proceeding.

(b) As used in this section:

(1) "Child abuse" has the same meaning as defined in Section 18951.

(2) "Multidisciplinary personnel" means a team as specified in Section 18951.

(3) "Child welfare services" means those services that are directed at preventing child abuse or neglect.

830.1. Notwithstanding any other provision of law, members of a juvenile justice multidisciplinary team engaged in the prevention, identification, and control of crime, including, but not limited to, criminal street gang activity, may disclose and exchange nonprivileged information and writings to and with one another relating to any incidents of juvenile crime, including criminal street gang activity, that may also be part of a juvenile court record or otherwise designated as confidential under state law if the member of the team having that information or writing reasonably believes it is generally relevant to the prevention, identification, or control of juvenile crime or criminal street gang activity. Every member of a juvenile justice multidisciplinary team who receives such information or writings shall be under the same privacy and confidentiality obligations and subject to the same penalties for violating those obligations as the person disclosing or providing the information or writings. The information obtained shall be maintained in a manner which ensures the protection of confidentiality.

As used in this section, "nonprivileged information" means any information not subject to a privilege pursuant to Division 8 (commencing with Section 900) of the Evidence Code.

As used in this section, "criminal street gang" has the same meaning as defined in Section 186.22 of the Penal Code.

As used in this section, "multidisciplinary team" means any team of three or more persons, the members of which are trained in the prevention, identification, and control of juvenile crime, including, but not limited to, criminal street gang activity, and are qualified to provide a broad range of services related to the problems posed by juvenile crime and criminal street gangs. The team may include, but is not limited to:

(a) Police officers or other law enforcement agents.

(b) Prosecutors.

(c) Probation officers.

(d) School district personnel with experience or training in

juvenile crime or criminal street gang control.

(e) Counseling personnel with experience or training in juvenile crime or criminal street gang control.

(f) State, county, city, or special district recreation specialists with experience or training in juvenile crime or criminal street gang control.

WELFARE AND INSTITUTIONS CODE
SECTION 10850-10853

10850. (a) Except as otherwise provided in this section, all applications and records concerning any individual made or kept by any public officer or agency in connection with the administration of any provision of this code relating to any form of public social services for which grants-in-aid are received by this state from the United States government shall be confidential, and shall not be open to examination for any purpose not directly connected with the administration of that program, or any investigation, prosecution, or criminal or civil proceeding conducted in connection with the administration of that program. The disclosure of any information that identifies by name or address any applicant for or recipient of these grants-in-aid to any committee or legislative body is prohibited, except as provided in subdivision (b).

(b) Except as otherwise provided in this section, no person shall publish or disclose or permit or cause to be published or disclosed any list of persons receiving public social services. Any county welfare department in this state may release lists of applicants for, or recipients of, public social services, to any other county welfare department or the State Department of Social Services, and these lists or any other records shall be released when requested by any county welfare department or the State Department of Social Services. These lists or other records shall only be used for purposes directly connected with the administration of public social services. Except for those purposes, no person shall publish, disclose, or use or permit or cause to be published, disclosed, or used any confidential information pertaining to an applicant or recipient.

(c) Any county welfare department and the State Department of Social Services shall provide any governmental entity that is authorized by law to conduct an audit or similar activity in connection with the administration of public social services, including any committee or legislative body so authorized, with access to any public social service applications and records described in subdivision (a) to the extent of the authorization. Those committees, legislative bodies, and other entities may only request or use these records for the purpose of investigating the administration of public social services, and shall not disclose the identity of any applicant or recipient except in the case of a criminal or civil proceeding conducted in connection with the administration of public social services.

(d) This section shall not prohibit the furnishing of this information to other public agencies to the extent required for verifying eligibility or for other purposes directly connected with the administration of public social services, or to county superintendents of schools or superintendents of school districts only as necessary for the administration of federally assisted programs providing assistance in cash or in-kind or services directly to individuals on the basis of need. Any person knowingly and intentionally violating this subdivision is guilty of a misdemeanor.

(e) In the context of a petition for the appointment of a conservator for a person who is receiving or has received aid from a public agency, as indicated above, or in the context of a criminal prosecution for a violation of Section 368 of the Penal Code both of the following shall apply:

(1) An adult protective services employee or ombudsman may answer truthfully at any proceeding related to the petition or prosecution, when asked if he or she is aware of information that he or she believes is related to the legal mental capacity of that aid recipient or the need for a conservatorship for that aid recipient. If the adult protective services employee or ombudsman states that he or she is aware of such information, the court may order the adult protective services employee or ombudsman to testify about his or her observations and to disclose all relevant agency records.

(2) The court may order the adult protective services employee or ombudsman to testify about his or her observations and to disclose any relevant agency records if the court has other independent reason to believe that the adult protective services employee or ombudsman has information that would facilitate the resolution of the matter.

(f) The State Department of Social Services may make rules and regulations governing the custody, use, and preservation of all records, papers, files, and communications pertaining to the administration of the laws relating to public social services under their jurisdiction. The rules and regulations shall be binding on all departments, officials and employees of the state, or of any political subdivision of the state and may provide for giving information to or exchanging information with agencies, public or political subdivisions of the state, and may provide for giving information to or exchanging information with agencies, public or private, that are engaged in planning, providing, or securing social services for or on behalf of recipients or applicants; and for making case records available for research purposes, provided that making these case records available will not result in the disclosure of the identity of applicants for or recipients of public social services and will not disclose any personal information in a manner that would link the information disclosed to the individual to whom it pertains, unless the department has complied with subdivision (t) of Section 1798.24 of the Civil Code.

(g) Any person, including every public officer and employee, who knowingly secures or possesses, other than in the course of official duty, an official list or a list compiled from official sources, published or disclosed in violation of this section, of persons who have applied for or who have been granted any form of public social services for which state or federal funds are made available to the counties is guilty of a misdemeanor.

(h) This section shall not be construed to prohibit an employee of a county welfare department from disclosing confidential information concerning a public social services applicant or recipient to a state or local law enforcement agency investigating or gathering information regarding a criminal act committed in a welfare department office, a criminal act against any county or state welfare worker, or any criminal act witnessed by any county or state welfare worker while involved in the administration of public social services at any location. Further, this section shall not be construed to prohibit an employee of a county welfare department from disclosing confidential information concerning a public social services applicant or recipient to a state or local law enforcement

agency investigating or gathering information regarding a criminal act intentionally committed by the applicant or recipient against any off-duty county or state welfare worker in retaliation for an act performed in the course of the welfare worker's duty when the person committing the offense knows or reasonably should know that the victim is a state or county welfare worker. These criminal acts shall include only those that are in violation of state or local law. Disclosure of confidential information pursuant to this subdivision shall be limited to the applicant's or recipient's name, physical description, and address.

(i) The provisions of this section shall be operative only to the extent permitted by federal law and shall not apply to, but exclude, Chapter 7 (commencing with Section 14000) and Chapter 8 (commencing with Section 14200) of this division, and for which a grant-in-aid is received by this state from the United States government pursuant to Title XIX of the federal Social Security Act (42 U.S.C. Sec. 1396 et seq.).

(j) (1) Public social services, as defined in Section 10051, includes publicly funded health care services administered or supervised by the department or the State Department of Health Care Services, except that, as used in this section, it does not include the Medi-Cal program. This subdivision does not affect or alter the exclusions contained in subdivision (i) or the confidentiality provisions contained in Section 14100.2.

(2) This subdivision clarifies existing law.

10850.1. (a) Notwithstanding any other provision of law, for purposes of Section 10850, the activities of a multidisciplinary personnel team engaged in the prevention, identification, management, or treatment of child abuse or neglect, or of the abuse of elder or dependent persons are activities performed in the administration of public social services, and a member of the team may disclose and exchange any information or writing that also is kept or maintained in connection with any program of public social services or otherwise designated as confidential under state law which he or she reasonably believes is relevant to the prevention, identification, management, or treatment of child abuse or neglect, or of the abuse of elder or dependent persons to other members of the team. All discussions relative to the disclosure or exchange of any such information or writing during team meetings are confidential and, notwithstanding any other provision of law, testimony concerning any such discussion is not admissible in any criminal, civil, or juvenile court proceeding.

(b) As used in this section:

(1) "Child abuse" has the same meaning as defined in Section 18951. As used in this section, "abuse of elder or dependent persons" has the meaning given in Section 15610.07.

(2) "Multidisciplinary personnel team" means a team as specified in Section 15610.55 relative to the abuse of elder or dependent persons or 18951 relative to child abuse or neglect.

10850.2. Notwithstanding the provisions of Section 10850, factual

information relating to eligibility provided solely by the public assistance recipient contained in applications and records made or kept by any public officer or agency in connection with the administration of any public assistance program shall be open for inspection by the recipient to which the information relates and by any other person authorized in writing by such recipient. The written authorization shall be dated and signed by such recipient and shall expire one year from the date of execution. In the event of any hearing under the provisions of this division, the attorney or authorized representative of the applicant or recipient shall be entitled to inspect the case record relating to the applicant or recipient prior to, as well as during, the hearing.

No list or names obtained through such access to such records or applications as provided in this section shall be used for any commercial or political purposes.

10850.3. (a) Notwithstanding Section 10850, an authorized employee of a county welfare department may disclose confidential information concerning a public social services applicant or recipient to any law enforcement agency where a warrant has been issued for the arrest of the applicant or recipient for the commission of a felony or a misdemeanor. Information that may be released pursuant to this section shall be limited to the name, address, telephone number, birth date, social security number, and physical description of the applicant for, or recipient of, public social services.

(b) A county welfare department may release the information specified by this section to any law enforcement agency only upon a written request from the agency specifying that a warrant of arrest for the commission of a felony or misdemeanor has been issued against the applicant or recipient. This request may be made only by the head of the law enforcement agency, or by an employee of the agency so authorized and identified by name and title by the head of the agency in writing to the county welfare department. A county welfare department shall notify all applicants of public social services that release of confidential information from their records will not be protected if a felony or misdemeanor arrest warrant is issued against the applicant. A recipient of public social services shall be notified, at the time of renewal of his or her application for public social services, that a release of confidential information can be made if a felony or misdemeanor arrest warrant is issued against the recipient.

(c) This section shall not be construed to authorize the release of a general list identifying individuals applying for or receiving public social services.

(d) The provisions of this section shall be operative only to the extent permitted by federal law. The section shall not apply to, but shall exclude, the Medi-Cal program, established pursuant to Chapter 7 (commencing with Section 14000) and following.

10850.31. (a) For the CalWORKs program and CalFresh only, notwithstanding any other provision of law, the address, social security number, and, if available, photograph of any applicant or recipient shall be made available, on request, to any federal, state,

or local law enforcement officer if the officer furnishes the county welfare department with the name of the applicant or recipient and notifies the county welfare department that the following apply:

(1) Any one of the following applies:

(A) The applicant or recipient is fleeing to avoid prosecution, custody, or confinement after conviction, for a crime that, under the law of the place the applicant is fleeing, is a felony, or, in the case of New Jersey, a high misdemeanor.

(B) The applicant or recipient is violating a condition of probation or parole imposed under state or federal law.

(C) The applicant or recipient has information that is necessary for the officer to conduct an official duty related to those issues stated in paragraph (1) or (2).

(2) Locating or apprehending the applicant or recipient is an official duty of the law enforcement officer.

(3) The request is being made in the proper exercise of an official duty.

(b) This section shall not authorize the release of a general list identifying individuals applying for or receiving public social services under the CalWORKs program or CalFresh.

(c) This section shall be implemented only to the extent permitted by federal law.

10850.4. (a) Within five business days of learning that a child fatality has occurred in the county and that there is a reasonable suspicion that the fatality was caused by abuse or neglect, the custodian of records for the county child welfare agency, upon request, shall release the following information:

(1) The age and gender of the child.

(2) The date of death.

(3) Whether the child was in foster care or in the home of his or her parent or guardian at the time of death.

(4) Whether an investigation is being conducted by a law enforcement agency or the county child welfare agency.

(b) All cases in which abuse or neglect leads to a child's death shall be subject to the disclosures required in subdivision (c). Abuse or neglect is determined to have led to a child's death if one or more of the following conditions are met:

(1) A county child protective services agency determines that the abuse or neglect was substantiated.

(2) A law enforcement investigation concludes that abuse or neglect occurred.

(3) A coroner or medical examiner concludes that the child who died had suffered abuse or neglect.

(c) Upon completion of the child abuse or neglect investigation into the child's death, as described in subdivision (b), the following documents from the juvenile case file shall be released by the custodian of records upon request, subject to the redactions set forth in subdivision (e):

(1) All of the information in subdivision (a).

(2) For cases in which the child's death occurred while living with a parent or guardian, all previous referrals of abuse or neglect of the deceased child while living with that parent or guardian shall be disclosed along with the following documents:

(A) The emergency response referral information form and the emergency response notice of referral disposition form completed by

the county child welfare agency relating to the abuse or neglect that caused the death of the child.

(B) Any cross reports completed by the county child welfare agency to law enforcement relating to the deceased child.

(C) All risk and safety assessments completed by the county child welfare services agency relating to the deceased child.

(D) All health care records of the deceased child, excluding mental health records, related to the child's death and previous injuries reflective of a pattern of abuse or neglect.

(E) Copies of police reports about the person against whom the child abuse or neglect was substantiated.

(3) For cases in which the child's death occurred while the child was in foster care, the following documents in addition to those specified in paragraphs (1) and (2) generated while the child was living in the foster care placement that was the placement at the time of the child's death:

(A) Records pertaining to the foster parents' initial licensing and renewals and type of license or licenses held, if in the case file.

(B) All reported licensing violations, including notices of action, if in the case file.

(C) Records of the training completed by the foster parents, if in the case file.

(d) The documents listed in subdivision (c) shall be released to the public by the custodian of records within 10 business days of the request or the disposition of the investigation, whichever is later.

(e) (1) Prior to releasing any document pursuant to subdivision (c), the custodian of records shall redact the following information:

(A) The names, addresses, telephone numbers, ethnicity, religion, or any other identifying information of any person or institution, other than the county or the State Department of Social Services, that is mentioned in the documents listed in paragraphs (2) and (3) of subdivision (c).

(B) Any information that would, after consultation with the district attorney, jeopardize a criminal investigation or proceeding.

(C) Any information that is privileged, confidential, or not subject to disclosure pursuant to any other state or federal law.

(2) (A) The State Department of Social Services shall promulgate a regulation listing the laws described in subparagraph (C) of paragraph (1) and setting forth standards governing redactions.

(B) Notwithstanding the rulemaking provisions of the Administrative Procedure Act (Chapter 3.5 (commencing with Section 11340) of Part 1 of Division 3 of Title 2 of the Government Code), until emergency regulations are filed with the Secretary of State, the State Department of Social Services may implement the changes made to Section 827 and this section at the 2007-08 Regular Session of the Legislature through all-county letters or similar instructions from the director. The department shall adopt as emergency regulations, as necessary to implement those changes, no later than January 1, 2009.

(C) The adoption of regulations pursuant to this paragraph shall be deemed to be an emergency necessary for the immediate preservation of the public peace, health, safety, or general welfare. The emergency regulations authorized by this section shall be exempt from review by the Office of Administrative Law. The emergency regulations authorized by this section shall be submitted for filing with the Secretary of State and shall remain in effect for no more

than 180 days, by which time the final regulations shall be adopted.

(f) Upon receiving a request for the documents listed in subdivision (c), the custodian of records shall notify and provide a copy of the request upon counsel for any child who is directly or indirectly connected to the juvenile case file. If counsel for a child, including the deceased child or any sibling of the deceased child, objects to the release of any part of the documents listed in paragraphs (2) and (3) of subdivision (c), they may petition the juvenile court for relief to prevent the release of any document or part of a document requested pursuant to paragraph (2) of subdivision (a) of Section 827.

(g) Documents from the juvenile case file, other than those listed in paragraphs (2) and (3) of subdivision (c), shall only be disclosed upon an order by the juvenile court pursuant to Section 827.

(h) Once documents pursuant to this section have been released by the custodian of records, the State Department of Social Services or the county welfare department or agency may comment on the case within the scope of the release.

(i) Information released by a custodian of records consistent with the requirements of this section does not require prior notice to any other individual.

(j) Each county welfare department or agency shall notify the State Department of Social Services of every child fatality that occurred within its jurisdiction that was the result of child abuse or neglect. Based on these notices and any other relevant information in the State Department of Social Services' possession, the department shall annually issue a report identifying the child fatalities and any systemic issues or patterns revealed by the notices and other relevant information. The State Department of Social Services, after consultation with interested stakeholders, shall provide instructions by an all-county letter regarding the procedure for notification.

(k) For purposes of this section, the following definitions apply:

(1) "Child abuse or neglect" has the same meaning as defined in Section 11165.6 of the Penal Code.

(2) "Custodian of records," for the purposes of this section and paragraph (2) of subdivision (a) of Section 827, means the county welfare department or agency.

(3) "Juvenile case files" or "case files" include any juvenile court files, as defined in Rule 5.552 of the California Rules of Court, and any county child welfare department or agency or State Department of Social Services records regardless of whether they are maintained electronically or in paper form.

(4) "Substantiated" has the same meaning as defined in Section 11165.12 of the Penal Code.

(l) A person disclosing juvenile case file information as required by this section shall not be subject to suit in civil or criminal proceedings for complying with the requirements of this section.

(m) This section shall apply only to deaths that occur on or after January 1, 2008.

(n) Nothing in this section shall require a custodian of records to retain documents beyond any date otherwise required by law.

(o) Nothing in this section shall be construed as requiring a custodian of records to obtain documents not in the case file.

10850.5. A county welfare department may, without the need to provide written documentation that consent has been obtained from a client, provide information to a housing authority created pursuant to Part 2 (commencing with Section 34200) of Division 24 of the Health and Safety Code, in order to aid the housing authority in the administration of that part. This section may be implemented either through an automated data exchange system or through a manual system. Any housing authority receiving and maintaining information pursuant to this section shall comply with confidentiality and privacy laws concerning the collection, maintenance, and dissemination of information, as contained in Section 10850 and the federal Privacy Act of 1974, contained in Section 552a of Title 5 of the United States Code. The county welfare department shall provide a written form to each person about whom information is to be provided to a housing authority pursuant to this section. The form shall notify the person that the information exchanges may occur. A copy of the form may be retained by the person and the county welfare department. The form shall specify the purpose for which the information has been solicited, the entities to which the information may be provided, the uses that may be made of the information, as set forth in Section 552a(e)(3) of Title 5 of the United States Code, and the right of the client to request review of the information that has been provided to the authority. The county welfare department may provide only information that is necessary to determine eligibility for housing authority programs or services for which the client has applied or which he or she is receiving. The county welfare department shall allow the client to review the information it has provided to a housing authority, upon request of the client. This section is not intended to eliminate any other legal obligation of the county welfare department to obtain consent from a client before releasing information to another entity.

10850.7. (a) Notwithstanding the provisions of Section 10850, an authorized employee of a county welfare department may disclose confidential information concerning a public social services applicant or recipient to any law enforcement agency where the applicant or recipient is deceased. Information that may be released pursuant to this section shall be limited to the name, address, telephone number, birthdate, social security number, and physical description of the applicant for, or recipient of, public social services.

A county welfare department may release the information specified by this section to any law enforcement agency only upon a written request from the head of the agency specifying that the applicant or recipient is deceased and that the agency is otherwise unable to adequately identify the deceased. The information specified may alternatively be released by telephone, whereupon the head of the law enforcement agency shall submit the request in writing within five days of the release.

(b) This section shall not be construed to authorize the release of a general list identifying individuals applying for or receiving public social services.

(c) The provisions of this section shall be operative only to the extent permitted by federal law. The section shall not apply to, but

shall exclude the Medi-Cal program established pursuant to Chapter 7 (commencing with Section 14000) and following.

10850.9. (a) Notwithstanding Section 10850, an authorized employee of a county social services department may disclose the name and residential address of elderly or disabled clients to police, fire, paramedical personnel, or other designated emergency services personnel, in the event of a public safety emergency that necessitates the possible evacuation of the area in which those elderly or disabled clients reside. Those public safety emergencies include, but are not limited to, fires, earthquakes, gas leaks, bomb scares, and other natural or human-made occurrences that jeopardize the immediate physical safety of county residents.

(b) The Director of Social Services shall seek any federal approval necessary to implement subdivision (a).

(c) Subdivision (a) shall be implemented only if the director executes a declaration, that shall be retained by the director, stating that any federal approval required for implementation of subdivision (a) has been obtained, and only for the duration of that approval.

CALIFORNIA PENAL CODE 502(c)
"COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"

(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) wrongfully 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 any 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 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.

DEPARTMENT OF HEALTH SERVICES
COUNTY OF LOS ANGELES

SUBJECT: WORKFORCE SECURITY

POLICY NO.: 935.03

PURPOSE: To ensure DHS workforce members have appropriate access to data systems and information contained in data systems and to prevent unauthorized access to confidential and Protected Health Information (PHI).

POLICY: It is the policy of the Department of Health Services (DHS) to ensure the security (confidentiality, integrity and availability) of PHI and other confidential information. DHS will develop and implement security procedures that protect the confidentiality of PHI and other confidential information. Access will be granted based upon the workforce member's job responsibility and "need to know".

DEFINITIONS: **PROTECTED HEALTH INFORMATION (PHI)** means individually identifiable information relating to past, present and future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

WORKFORCE MEMBERS means employees, volunteers, trainees, and other persons whose conduct in the performance of work for the department, its offices, programs or facilities, is under the direct control of the department, office, program or facility, regardless of whether they are paid by the entity.

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

PROCEDURES: DHS Facility CIOs/designees must work with DHS facility System Managers/Owners and Human Resources to develop and coordinate implementation of the workforce security procedures.

DHS Workforce Authorization and Supervision Procedure

DHS facility System Managers/Owners must ensure that workforce members are granted access authorization in accordance with DHS Policy 935.04, Information Access Management

APPROVED BY:

EFFECTIVE DATE: March 1, 2005

SUPERSEDES:

The Authorization and supervision process must consist of the following components:

1. DHS facility managers/supervisors must identify and supervise workforce members who work with or have access to PHI and other confidential information. DHS facility managers/supervisors must identify the minimum information access required by these workforce members to do their job.

2. DHS facility System Managers/Owners or designees must identify the security levels necessary for securing the system and allow workforce members to perform their jobs. DHS facility System Managers/Owners will assign workforce members to the minimum security level that they need to perform their job function.

3. DHS facility managers/supervisors must restrict access to PHI and other confidential information by unauthorized workforce members.

4. DHS facility managers/supervisors must provide authorization and supervision to workforce members and others who need to be in areas where PHI and other confidential information may be accessed and take appropriate safeguards to ensure those who may be exposed to PHI and other confidential information are made aware of the policies protecting that information.

DHS Workforce Clearance Procedure

DHS facility System Managers/Owners must ensure that workforce members' access to PHI and other confidential information is limited to the minimum necessary to perform their job responsibilities.

The clearance process must consist of the following components:

1. DHS facility System Manager/Owner or designee must work with Human Resources (HR) to ensure proper workforce clearance procedures are implemented. Refer to DHS Policy No. 703.1, Criminal Records Background Check/Fingerprinting Policy.

2. DHS facility System Managers/Owners or designees must ensure all applications for access to a system are complete and approved by the appropriate workforce managers/supervisors. They must also ensure that each workforce member with access has signed the County Acceptable Use Policy agreement and an acknowledgment of DHS Policy No. 935.20, Acceptable Use Policy for County Information Technology Resources that defines their responsibility for the protection of the confidentiality, integrity and availability of all DHS information resources and restrictions for utilizing those resources. DHS Human Resources must ensure that each new workforce member receives and signs the County Acceptable Use Policy agreement and an acknowledgment of DHS Policy No. 935.20 during the new hire orientation and that each workforce member completes the agreement and the acknowledgment during the annual Performance Evaluation process. The signed agreement and acknowledgment will be filed in the workforce member's official personnel folder.

DHS Workforce Termination Procedure (Access)

DHS facility System Managers/Owners must ensure that departing workforce members' access to all PHI and other confidential information is terminated upon termination of employment.

The termination process must consist of the following components:

1. DHS facility System Managers/Owners must be notified by the workforce member's Supervisor as soon as possible, but in no circumstance later than the day the workforce member's employment or other service arrangement with DHS ends.

2. DHS facility System Managers/Owners must be notified by the workforce member's Supervisor when a workforce member's status/function/responsibility has changed. DHS facility System Managers/Owners must promptly review the workforce member's access to PHI and other confidential information and must modify the member's access as needed.

3. DHS facility System Managers/Owners must terminate the workforce member's access to PHI or other confidential information upon notification by the workforce member's supervisor when the workforce member terminates employment or transfers to another facility or County department. Access termination must be:

   a. As soon as possible but in no circumstance later than 5 business days when the end of employment is voluntary.
   b. As soon as possible but in no circumstance later than close of the same business day or end of workforce member's work shift when the end of employment is involuntary,

AUTHORITY: 45 Code of Federal Regulations, Part 164, Subpart C, Section 164.308 (a)(3)(ii)
Board of Supervisors Policy Nos.:
6.100, "Information Technology and Security Policy"
6.101, "Use of County Information Technology Resources"

CROSS REFERENCES: DHS Policies:

361.8,	"Minimum Necessary Requirements for Use and Disclosure of Protected Health Information (PHI)"
703.1,	"Criminal Records Background Check/Fingerprinting Policy"
935.20,	"Acceptable Use Policy for County Information Technology Resources"

Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: SECURITY INCIDENT REPORT AND RESPONSE

POLICY NO: 935.06

PURPOSE:

To establish a policy to protect the integrity, availability and confidentiality of confidential or proprietary information, including electronic Protected Health Information (ePHI). and to outline Department of Health Services (DHS') coordinated response to electronic communication systems incidents.

POLICY:

It is the DHS' policy to protect electronic confidential and patient information in compliance with state and federal laws, as well as the DHS' policies and business practices for identifying, tracking and responding to network and computer-based IT Security Incidents.

DHS Workforce Members are required to immediately report any actual or suspected security incidents, intrusion attempts, security breaches, theft or loss of hardware and other security related incidents which violate the confidentiality, integrity, or availability of digital information to the facilities Information Technology (IT) Department. Incidents must be reported to the facility IT service desk, facility information security coordinator, facility privacy coordinator, and to the DHS' Security Compliance Division at SecurityCompliance@dhs.lacounty.gov.

Upon notification of an incident the Security and Compliance Division will investigate and, as needed, escalate, remediate, or refer to others. The incident will be documented by providing a general description of events, approximate timelines, the parties involved, resolution of the incident, external notifications required and recommendations for prevention and remediation.

The Departmental Information Security Officer (DISO) or designee and Departmental Computer Emergency Response Team (DCERT) are responsible for determining the appropriate level of response to a security incident. Facility Chief Information Officers (CIOs) must ensure that the System Managers/Owners respond in a manner authorized and directed by the DISO or designee and DCERT.

The DHS security incident reporting and response procedures are to be followed, including the completion of the DHS Incident Report form. This is consistent with Board of Supervisor's Policy No. 6.103, Countywide Computer Security Threat Response.

APPROVED BY:

REVIEW DATES:

EFFECTIVE DATE: September 30, 2009

SUPERSEDES: January 1, 2006

SUBJECT: SECURITY INCIDENT REPORT AND RESPONSE

POLICY NO.: 935.06

DEFINITIONS:

IT Security Incident ("Incident") means any activity that harms or represents a serious threat to the whole or part of the Department of Health Services computer, and network-based resource(s) such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure, change or deletion of PHI, or a crime or natural disaster that destroys access to or control of these resources. (Refer to Incident Reporting Process Flow (Attachment I) and IT Security Incident Response Matrix (Attachment II)).

CCERT Countywide Computer Emergency Response Team has the responsibility of responding and reporting Information Technology (IT) security incidents within the County

DCERT Department's Computer Emergency Response Team has the responsibility of responding and reporting IT security incidents within DHS

FISC Facility Information Security Coordinator

INFORMATION TECHNOLOGY (IT) refers to the study, design, development, implementation, support and/or management of computer-based information systems, particularly software application and computer hardware.

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

PROCEDURE:

As required by the Policy section above, suspected and actual breaches of security must be reported to the DHS facility IT service desk. The facility IT service desk will contact the FISC or the facility DCERT who will complete and submit a Security Incident Report (Attachment III to the DHS Security Compliance Division.

The process for information security incident includes:

- Identify and report the incident
- Validate the incident
- Evaluate the incident for the extent of its threat

- Take actions based on prioritization of assets and processes
- Re-evaluate and repeat actions until threat is controlled
- Inform workforce members and management, as necessary
- Document details, as appropriate
- Initiate long-term actions to reduce likelihood of recurrence, as appropriate.

Workforce members must report all potential information security incidents to the appropriate management personnel. A workforce member may not prohibit or otherwise attempt to hinder or prevent another workforce member from reporting an information security incident. Incidents may also be identified through automated processes such as periodic virus scans, intrusion detection analysis, firewall and other log analysis, and other appropriate audit mechanisms.

AUTHORITY:

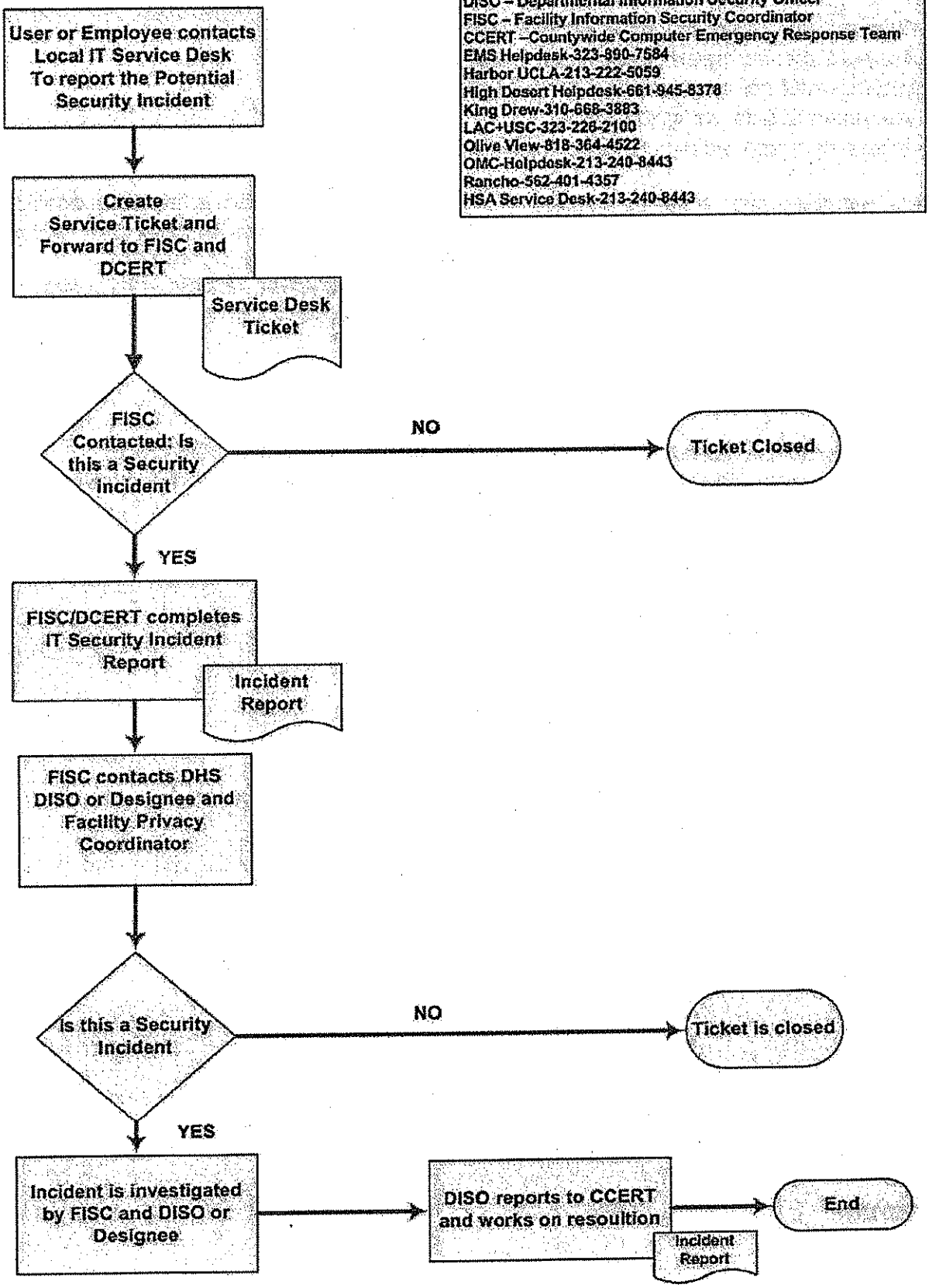
45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.308(a)(6)(i)
Board of Supervisors Policy No. 6.103, "Countywide Computer Security Threat response.

ATTACHMENT I

DHS IT Security Incident Reporting Process Flow

Health Services

DISO – Departmental Information Security Officer
FISC – Facility Information Security Coordinator
CCERT – Countywide Computer Emergency Response Team
EMS Helpdesk-323-890-7584
Harbor UCLA-213-222-5059
High Desert Helpdesk-661-945-8378
King Drew-310-668-3883
LAC+USC-323-226-2100
Olive View-818-364-4522
OMC-Helpdesk-213-240-8443
Rancho-562-401-4357
HSA Service Desk-213-240-8443



ATTACHMENT II

SECURITY INCIDENT RESPONSE MATRIX

IT Security Incidents			
IT Security Incident - The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.			
Incident Type	Name	Description of Incident	Reporting Timeframe
Incident 1	Theft	Any type of theft of an IT resource. Including software, hardware, PC's laptops or phones.	Immediately
Incident 2	Unauthorized Access	Any type of un-authorized access to a secure are containing any IT resource or asset.	Within 24 hours
Incident 3	Denial of Service	Any attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This includes being the victim or participating in the DoS.	Immediately
Incident 4	Malicious Code Execution	Any successsful installation of malicious software (e.g.,virus, worm, trojan horse or other code based malicious entity) that infects an operating system or application.	Within 24 hours
Incident 5	Improper Usage	A person violates acceptable computing use policies.	Within 5 days
Incident 6	Scans/Probes/Attempted Access	Any activity that seeks to access or identify a computer, open ports, protocols, service or any combination for later exploit.	Within 5 days
Incident 7	Service Unavailable	When any service or application (e.g., email, internet, Affinity) is unavailble for use over a period of time.	Within 24 hours

ATTACHMENT III

Department of Health Services
Security Compliance Division
IT Security Incident Report

Health Services
LOS ANGELES COUNTY

Contact Information

Facility Name:		Department or Division Location
Contact name:	Phone #: ( )	Email address:

Incident Information

Date incident *occurred*:	Date incident *discovered*:	#Machines affected:
Time incident *occurred*:	Time incident *discovered*:	

Type 1 Incident:

System Compromise/Intrusion
- ☐ Root Compromise ☐ User Compromise

Loss, Theft, or Missing
- ☐ Desktop ☐ Laptop ☐ Media ☐ Other (please specify)

Malicious Code
- ☐ Trojan ☐ Virus ☐ Worm ☐ Other (please specify)

- ☐ Web Site Defacement
- ☐ Denial of Service
- ☐ Critical Infrastructure Protection
- ☐ Unauthorized Use
- ☐ Information Compromise

Type 2 Incident:
- ☐ Attempted Intrusion
- ☐ Reconnaissance Activity

Security Category:
- ☐ Low Security Category: *limited* adverse affect
- ☐ Moderate Security Category: *serious* adverse affect
- ☐ High Security Category: *severe or catastrophic* adverse effect

Information sensitivity:
- ☐ PHI or ePHI
- ☐ Other (please specify)

Which critical infrastructure was affected, if any?

☐ Facility Privacy Coordinator Contacted? (Name & Phone#)

IP address of affected machine(s):	Domain name of affected machine(s):
Operating system(s) of affected machine(s):	Last time the affected machine(s) patched:
Functions of affected machine(s):	Application software affected:

Description of incident:

Method of detection:

What security infrastructure was in place:

IP address(es) of attackers:	Destination Port(s) and Protocol(s):
Domain name(s) of attacker(s):	Country(ies) of attacker(s):

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	Evidence of spoofing:

Other information:

Impact and Actions Taken

Assessment of the impact of the incident:

Did the intrusion damage any machine(s): ☐ Yes ☐ No If yes, please describe:

What actions have been taken:

Other Information

Who has been notified?
- ☐ DHS Security Compliance Division
- ☐ Other Agencies (please specify)
- ☐ HSA Helpdesk

If PHI is involved, have affected people been notified?

Report Information (Call Center Use Only)

Report Date:	Report Time:	Facility Help Desk Ticket #: HSA Help Desk Ticket #:

Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: PHYSICAL ACCESS CONTROL AND VALIDATION

POLICY NO: 935.10

PURPOSE:

The purpose of this policy is to define the requirements for the physical protection of Department of Health Services' (DHS') information systems, data, and related assets.

POLICY:

Physical security controls must be implemented to protect all DHS facilities and areas in which sensitive information systems and data (e.g., ePHI) are located. The types of physical security controls implemented must commensurate with the level of risk associated with the particular Information Technology (IT) facility/area.

Access Requisition & Approval – A formalized process must be implemented for requesting and approving workforce member access to sensitive IT facilities/areas. A history of all approved access requests must be maintained for audit trail purposes.

Workforce Access – Physical access to facilities/areas containing sensitive information systems, data, and related assets must be restricted to workforce members; such access must be based upon business-need.

Visitor Access – All visitor access must be tracked. Visitors include non-authorized workforce members, vendors, and maintenance support personnel. An authorized workforce member must be present when a visitor requires access to an IT facility/area. IT-related items entering or exiting the facility/area must be documented.

Access Controls – Facilities and areas that house sensitive information systems, data, and related assets must be made physically sound. Access controls, such as card-key systems, combination locks, biometrics, etc. must be implemented on all ingress and egress points to prevent unauthorized access.

Monitoring – Based upon the sensitivity of the IT facility/area, monitoring capabilities should be considered. This may include implementation of video cameras and/or access control devices that log ingress and egress events. Data centers are a typical candidate for this type of control.

APPROVED BY: 

EFFECTIVE DATE: January 1, 2009

REVIEW DATES:

SUPERSEDES: January 1, 2005.
Facility Access Control

Access Reviews – A review of all personnel with physical access to restricted IT facilities/areas must be performed on at least a quarterly basis. The review must be documented for audit trail purposes. The person designated to approve access requests to the particular IT facility/area is responsible for this quarterly physical access review.

Validation – The Departmental Information Security Officer (DISO) or designee is responsible for performing announced or unannounced on-site reviews of physical access controls and related processes for each IT facility.

DEFINITIONS:

Ingress - An entry point.

Egress - An exit point.

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

AUTHORITY:

45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.310(a)(1) and (a)(2)(iii) – HIPAA Security Rule, Physical Safeguards, Facility Access Control, Access Control and Validation Procedures (A)

Board of Supervisors Policy 6.106, Physical Security

CROSS REFERENCE:

DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI)

Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: WORKSTATION & MOBILE DEVICE USE AND SECURITY POLICY

POLICY NO: 935.11

PURPOSE:

To restrict workstation use and access to Protected Health Information (PHI) and other confidential information by using physical, administrative, and technical controls.

POLICY:

Department of Health Services (DHS) must ensure workstation security procedures are enforced within each Facility. "Workstations" include County and personal computers, laptops and other mobile devices (e.g., tablet PCs, PDAs, computer carts), modems, printers, and fax machines, etc. that are used for County business.

1. All Users must use workstations and mobile devices in a manner commensurate with the sensitivity of the Information accessed from the workstations.

2. All Users must take reasonable physical security precautions to prevent unauthorized physical access to sensitive Information from workstations and mobile devices, (including Smartphones, Tablets and any Personally Owned Device). These precautions include taking into consideration the physical attributes of the surroundings (e.g., concealing video displays and securing unattended workstations).

3. DHS System Managers/Owners must implement physical safeguards to permit only authorized User access to workstations and mobile devices with accessibility to confidential and/or sensitive Information.

4. Only DHS supplied and supported workstations and mobile devices may be connected to DHS systems and access DHS data. Exceptions to this may include remote access required by vendors and business partners for support purposes and devices approved by the DHS CIO or designee.

5. Each Facility Help Desk must implement a process to make positive identification of individuals requesting password resets due to forgotten passwords.

All Users who use workstations and mobile devices as described above must be trained to exercise proper security practices. Training and documentation must be in accordance with

APPROVED BY: **EFFECTIVE DATE:** March 15, 2013

REVIEW DATES: **SUPERSEDES:** January 1, 2009

the DHS Policy No. 361.1, DHS Privacy and Security Compliance Program policies and procedures, including DHS Policy No. 361.24, Privacy and Security Training Policy, and DHS Policy No. 935.19, Data Security Documentation Requirement.

DEFINITIONS:

PROTECTED HEALTH INFORMATION (PHI) means individually identifiable information relating to past, present and future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

WORKFORCE MEMBER Employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DHS, is under its direct control whether or not they receive compensation from the County.

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

PROCEDURE:

Each Facility Chief Information Officer (CIO)/designee must ensure that the following workstation security procedures are implemented within each DHS Facility. "Workstations" include County and personal computers, mobile devices (e.g., tablet PCs, PDAs, Smartphones and computer carts), modems, printers, fax machines, etc., that are used for County business.

I. Workstation Use

These procedures are intended to include documented instructions delineating the proper functions to be performed by DHS workforce members and the manner in which those functions are to be performed (e.g., logging off before leaving a workstation unattended) to maximize the security of health information.

A. Access and Use of Workstation and Network Services
Measures to limit unauthorized access must include the following:

1. Configuration of workstations and network services.

a. Facility System Managers/Owners must configure workstations and network services to allow only authorized access to the workstation and network services (e.g., data, applications, intranet and Internet).

b. Workforce members must have authorization to access a workstation and the appropriate rights to do so. Users must not access any confidential and/or sensitive information from a workstation unless they have authorization to do so and it is necessary for doing their job.

2. Permitting only authorized access to workstations and network services through the use of controls.

   Each Facility CIO/designee, taking into consideration each system's Risk Analysis Sensitivity Score, DHS Policy No. 935.01, Information Security Management, is responsible for the creation, design and implementation of measures to limit unauthorized access by workforce members to workstations and network services.

   a. Unique User IDs and Passwords

      i. The Facility CIO/designee is responsible for ensuring the assignment of a unique user ID to each User, to identify and track the User's identity when logging into workstations, networks or applications.

      ii. Each User must protect his/her password. Users must not write down their password and place it at or near the workstation (e.g., a note taped to the monitor or placed under the keyboard).

      iii. Logging into workstations, networks or applications with another User's ID and/or password is prohibited.

      iv. Users must not share their unique User IDs (logon/system identifier) with any other person.

      v. Users' passwords must be changed at least once every ninety (90) days.

      vi. Passwords must be at least eight (8) characters and contain a combination of alpha and numeric characters.

b. Other User Authentication Methods

With authorization from the DHS Departmental Information Security Officer (DISO), Facility CIOs may utilize other User authentication methods (e.g., badge readers, biometric devices, tokens).

c. Password Reset Requests (forgotten passwords)

Some form of personal information must be used to positively identify a user prior to executing a password reset request (e.g., ID badge, online challenge question, preset (Personal Identification Number (PIN)), etc.

3. Access to Workstations Not in Use

a. Workstations not in use must be password protected and locked.

b. Workstations must be setup to generate a password protected screen saver when the computer receives no input for a specified period of time (to be determined by each Facility CIO based on result of risk assessment). Other "lockout" schemes that protect against the unauthorized access to confidential and/or sensitive information may be approved by the Facility CIO/designee.

4. Workstations must display an appropriate warning banner prior to gaining operating system access.

II. Access and Use of Mobile Devices

A. All mobile devices connected to DHS systems or accessing DHS data must be supplied and managed by DHS/Facility Information Technology (IT) departments. In the case of personally owned devices, the device owner must receive prior approval from the DHS CIO, or designee, to connect to the DHS network. The applicable technical support group at each facility will manage the maintenance of all mobile devices that connect to the DHS networks. Users of personal devices synced to the DHS network must sign and agree to the provisions of the department's Workstation & Mobile Device Use and Security Policy and it's corresponding Terms and Acceptable Use Agreement/Wipe Waiver Agreement (Attachment I), which states in part:

1. The choice to use the workforce member's personally owned mobile device is a personal choice and not ordered by the workforce member's supervisor.

2. Not all personal mobile devices are compatible with the County email system and only compatible devices will be allowed to access the DHS network. DHS-IT will not assist in determining, nor guarantee that a personal mobile device is compatible with the County email system.

3. The workforce member agrees that any configuration changes to a personal mobile device are the responsibility of the workforce member. DHS-IT will provide no technical support of personal mobile devices, and will provide no warranty, guarantee, or support should a personal mobile device experience functional problems or become inoperable.

4. The workforce member is fully responsible for the purchase, maintenance, and backup of a personal mobile device and for all monthly carrier data charges, if applicable. It is understood that DHS is not liable in any way for any device (hardware and software), or for any data and overage charges the workforce member may accrue due to syncing their personal mobile device to the County email system.

5. The workforce member agrees to password-protect the personal mobile device and to secure the device at all times.

6. The workforce member agrees to immediately notify DHS-IT if their personal mobile device is lost or stolen and file a security incident report by the end of the next business day. They must also agree to have DHS-IT and/or their wireless carrier remotely wipe/delete data on the personal mobile device. This will permanently erase all email, contacts, calendar, applications, and any/all other data stored on the device. This will reset the personal mobile device back to its factory default settings.

7. The workforce member agrees that by connecting their personal mobile device to the County email system, they are agreeing to cooperate with any legal hold, audit, or data discovery request from counsel, which may include an investigative search of all the data on, and possible confiscation of, the device.

8. The workforce member shall not use the personal mobile device to store confidential or sensitive data when sanctioned by federal (e.g. HIPAA/HITECH, Welfare Institutions Code), state, and/or local government legislation. The workforce member acknowledges that this privilege can be revoked by DHS management at any time.

B. Workforce members must exercise good judgment in determining the amount of necessary data stored on their mobile devices to perform their functions, as the security risk to such data is increased.

C. Access to mobile devices must be protected at all times consistent with the procedures set forth in the Access and Use of Mobile Devices section above.

D. Mobile devices containing sensitive information (e.g., confidential patient information) must be encrypted.

E. Use of personal USB drives (aka thumb drives) or other removable storage devices will be limited to read-only access while connected to a DHS workstation. To ensure proper data security, only DHS standard issued USB drives that are encrypted will be permitted read/write access while connected to a DHS workstation. The only exception to this policy may be in the case that DHS IT has approved and implemented security features on a workstation to ensure the adequate encryption of any personal USB drive device that may be connected to the workstation.

F. When traveling, a workforce member must not leave mobile devices unattended in non-secure areas.

G. Mobile devices left in cars must be stored out-of-sight and the car must be locked.

III. Physical Attributes of Surroundings

Workforce members must be aware of the physical attributes of the surroundings where the workstation is located. Precautions need to be taken to prevent unauthorized access to unattended workstations; to automatically erase sensitive information left displayed on unattended workstations; and to limit the ability of an unauthorized individual to observe sensitive information when a workstation is in use by a User. The following measures must be taken:

A. Confidential data (e.g., patient information) must be password protected, encrypted or stored on a secure network drive.

B. Confidential data having a Sensitivity Score of "High" must be encrypted.

C. Confidential data must not be downloaded without authorization from the Facility CIO/designee.

D. Confidential data must not be saved on removable devices (e.g., floppy disk, CD-ROM, external drives, USB drives) without proper safeguards and authorization from the Facility CIO/designee.

E. Removable media containing confidential data (e.g., patient information) must be maintained and stored in secured areas.

F. Printers are not to be left unattended in non-secure areas when printing confidential and/or sensitive information.

G. Disposal of confidential electronic records stored on removable or external media (e.g., CD-ROM, diskettes, hard drives) must be in accordance with DHS Policy No. 935.13, Device and Media Controls.

H. Use caution when viewing and entering confidential information.

I. Layout and design of the space must shield the view of the workstation screen from the public, unless the user complies with requirements of subsection III.J.

J. Where it is not possible, through layout and design of the space, to shield the workstation screen from view, devices like privacy screens and shields are to be used.

IV. Workstation Security

These procedures are intended to put in place physical safeguards to restrict access to information through securing DHS workstations and laptops.

A. General

1. Workstations located in public or open areas must be physically secured in a locked room, locked cabinets, or strongly anchored to deter unauthorized movement. Security cameras or additional forms of monitoring should be considered in high-risk areas.

2. Users are required to secure laptop computers with a cable lock if the system is maintained or left in an insecure location. Additionally, users are required to adequately secure and monitor laptops while in transit (e.g., airports, in vehicles, etc.).

3. Mobile devices must be secured when not in use. These devices must either be carried on persons or must be stored in secured areas.

4. Workstation equipment must not be removed from the premises unless documented and pre-approved by the User's supervisor.

5. Devices must be located in environments that are in accordance with the equipment manufacturer's operational specifications.

6. Inventory and maintenance records must be maintained for all workstations.

7. Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation in accordance with DHS Policy No. 361.23, Safeguards for Protected Health Information (PHI).

B. Hardware/Software

1. Workstations must be configured to require authentication (e.g., user ID and password) prior to users accessing system functions or data.

2. Workstations must be configured to store data to the network by default, as opposed to the user's local hard drive. Any sensitive data (e.g., ePHI) that must be stored locally on a mobile device must be approved and documented by DHS management.

3. All mobile devices (e.g., laptops, Blackberries, PDAs, and Smartphones etc.) must be secured with full disk encryption to prevent disclosure of any data that may be stored on the system.

4. Workstation settings must be configured to implement automatic screen locking after 30 minutes of inactivity. DHS IT management approval and documentation is required where specific business processes call for an inactivity setting set for a longer period of time.

5. Users are required to initiate the workstation screen-lock feature when stepping away from the system for short periods of time; users should log off for extended

periods away from workstations. The screen-lock function is typically instituted by pressing the CTRL-ALT-DEL key sequence, then selecting "lock workstation."

6. Personal firewalls must be enabled on all laptops. Laptops are commonly connected to non-DHS networks (e.g., home networks, hotel networks, etc.) and thus, not protected by the security controls in place on the DHS network. Personal firewalls will help ensure that laptops are not compromised while connected to non-DHS networks.

7. Workforce members must not change the system configuration of their workstation without proper authorization (e.g., network properties, video card).

8. Workforce members must not install or uninstall software on their workstation without proper authorization and licensing (e.g., downloaded Internet software, games, patches, plug-ins, screen savers).

9. Only authorized Users may install/uninstall software and perform repair services on workstations.

10. Workforce members must not re-enable floppy drives, CD-ROM drives, USB ports, etc., on workstations that have access to confidential data, unless the workforce member is authorized to use those drives.

11. The Facility CIO/designee must ensure appropriate controls are in place when sending equipment off premises for maintenance (i.e., maintenance contract must include business associate language).

12. All hardware and software connected to a Facility's network services must be managed centrally within each Facility.

AUTHORITY:

45 Code of Federal Regulations, Part 164, Subpart C, Section 164.310(a)(2)(iv)(b) and (c)
Board of Supervisors Policies:
- 6.100, Information Technology and Security Policy
- 6.101, Use of County Information Technology
- 6.102, Countywide Antivirus Security Policy
- 6.106, Physical Security

CROSS REFERENCES:

Administrative Controls:
DHS Policy No. 935.03, Workforce Security

Technical Controls:
DHS Policy No. 935.14, System Access Control

DHS Policies:
361.23, Safeguards for Protected Health Information (PHI)
361.24, Privacy and Security Awareness and Training Policy
935.01, Information Security Management
935.13, Device and Media Controls
935.17, Person or Entity Authentication
935.19, Data Security Documentation Requirement

DEPARTMENT OF HEALTH SERVICES
PERSONAL ELECTRONIC COMMUNICATION DEVICES PROGRAM

Terms and Acceptable Use Agreement / Wipe Waiver Agreement

At the discretion of the department head or his/her designee, workforce members who have a business need for mobile device (Smartphones, etc.) service and/or remote access to their Department of Health Services (DHS) email, network files and other information resources may be authorized to use a personal phone, smartphone or tablet device in lieu of a department-issued device. Workforce members authorized by management to participate in this program must agree and adhere to the following terms and conditions:

1. Participation in this program is voluntary and may be terminated by the workforce member and/or the department at any time, for any reason.

2. Any personal phone, smartphone, tablet or other similar device (air card, broadband card, etc.) used pursuant to this program shall be expressly defined as the personal property and sole responsibility of the workforce member. The department assumes no liability for damage, loss or theft of the workforce member's device, under any circumstances.

3. Participants will be solely responsible for the costs of private ownership, including but not limited to the purchase, activation, maintenance, support, monthly usage, late fees, interest, term commitment obligations and replacement of such devices, as well as any increase in personal income tax liability. The participant shall pay any costs to maintain service coverage.

4. DHS is not liable for the loss or corruption of personal data on the workforce member's device, loss of use, or any repairs or maintenance arising from the use of the device for department business. Updates to, maintenance, repair and replacement of the device are the sole responsibility of the participant.

5. Participants must report to their management/departmental designee, within one business day, when the following events take place:
   a. Whenever any personal device used pursuant to this program is suspected or known to be lost or stolen;
   b. Participants terminate employment with or retire from DHS;
   c. Participants' job responsibilities changed and is no longer eligible to participate in the program;
   d. Participants change/transfer position that is not eligible to participate in the program; or
   e. Participants elect to stop participation in the program.

   Upon notification of loss/theft or change in status as indicated above, DHS may initiate a remote wipe of the device to ensure that Department-related data is safeguarded. Participants consent to remote wiping when one of the events listed above has taken place and remote wiping is deemed necessary by the department. Participants also agree DHS will not be liable for any personal data loss. When the remote wipe command is issued, all data including personal data such as contacts, apps, picture/data files, etc. may be deleted and the device may be restored to factory default settings.

6. Participants understand that Department-related data and correspondence accessed or received via the personal device may be subject to disclosure pursuant to the California Public Records Act, and may also be compelled via a discovery request, subpoena or other legal process. In addition, in some cases, personal email transmissions may also be subject to such disclosure.

7. Participants must adhere to DHS policies, the Board of Supervisors policies (BOS) and the County's Mobile Device Security Standards with respect to DHS-related data, correspondence and communications accessed, transmitted, received or stored on the participant's device:

    a. BOS 6.100 Information Technology and Security Policy
    b. BOS 6.101 Use of County Information Technology Resources (County Acceptable Use Agreement)
    c. BOS 6.102 Countywide Antivirus Security Policy
    d. BOS 6.104 Use of Electronic Mail by County Employees
    e. BOS 6.105 Internet Usage Policy
    f. BOS 6.109 Security Incident Reporting
    g. BOS 6.110 Protection of Information on Portable Computing Devices
    h. BOS 6.112 Secure Deposition of Computing Devices
    i. Chief Information Office-Smartphone Security and Privacy Requirements Standard
    j. Chief Information Office-Portable Device Strategy
    k. DHS 935.00 DHS Information Technology and Security Policy
    l. DHS 935.20 Acceptable Use of County Information Technology Resources
    m. DHS 935.11 Workstation & Mobile Device Use and Security Policy
    n. DHS 935.06 Security Incident Report and Response

8. DHS reserves the right to inspect, at any time and without prior notice, any personal device connected to any DHS mobile enterprise servers such as BlackBerry Enterprise Server (BES) or Microsoft Exchange ActiveSync (AS) server. Other inspections shall be in accordance with Board-adopted and DHS Information Technology Security Policies.

9. Participants must not allow others to use or access DHS resources/data via their personal device(s).

10. Participants must activate a password lock and autolock (30 minute maximum), and shall not disable it at any time.

11. Participants must not use personal devices connected to DHS networks or information resources for illegal activity.

12. Participants must provide documentation to the department coordinator, when requested, to verify continued ownership and business use of a personal mobile device.

13. Participants must submit to their management/departmental designee or department coordinator a revised Mobile Device Activation Form, when they:
    a. Change or terminate cellular carriers
    b. Replace or retire their mobile device
    c. Sell or transfer device to another individual

    Participants are required to bring the old device to their IT department and perform the data wipe procedure in the presence of the Departmental Information Security Officer (DISO) or designee to ensure that all DHS confidential/sensitive data is properly sanitized.

14. Participants must disable Bluetooth pairing/discovery when not in use.

15. Participants must not store DHS data on a memory card (e.g., MicroSD card) used in the portable device.

The participant acknowledges that they have read, understand and agree to abide by the terms and conditions stated above. Participants who violate these terms and conditions will be disconnected from the mobile enterprise servers such as BES or AS and may be subject to disciplinary action. I understand that this agreement will be placed in my official personnel folder.

Workforce Member Name (Print)	Workforce Member Emp#/County ID#
Workforce Member Signature	Date

Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: SYSTEM ACCESS CONTROL

POLICY NO: 935.14

PURPOSE:

To preserve and protect the confidentiality, integrity and availability of the Department of Health Services (DHS) networks, systems and applications, all access to the Information Technology Assets/Resources are permitted only to those persons or software programs that have been granted access rights.

POLICY:

DHS Facility CIOs/designees must ensure that DHS facility System Managers/Owners implement the appropriate technical access control safeguards to allow DHS electronic information systems access only to those persons or software programs that have been granted access rights:

a. Unique User Identification. DHS systems must assign a unique name and/or number to each user for identifying and tracking user identity.

   Configure systems to track individual activity by user identification and record such activities as required by DHS Policy No. 935.15, System Audit Controls.

b. System Log-in Banner. Every login process for multi-user computers must include a special notice. This notice must state:

   (1) the system is to be used only by authorized users, and
   (2) by continuing to use the system, the user represents that he/she is an authorized user.

c. System Log-in Monitoring. User and process access to system must be recorded and monitored for successful and failed attempts.

d. Emergency Access Procedure. DHS systems must have alternate secured manual or automated procedures for accessing stored information during an emergency to be invoked by the DISO or designee when the usual means of secured access is not available.

APPROVED BY: [signature] **EFFECTIVE DATE:** December 1, 2010
REVIEW DATES: **SUPERSEDES:** March 1, 2005

e. Automatic Logoff. DHS Facility CIOs/designees must ensure that the DHS facility System Managers/Owners address the use of an automated process to terminate an electronic session after a predetermined time of inactivity.

f. Encryption/Decryption. DHS Facility CIOs/designees must ensure that DHS facility System Managers/Owners address the appropriate encryption for protecting electronic information contained within the storage structure for all DHS electronic data storage systems (i.e., databases or file systems) based on the DHS Facility Master Security Management Report in DHS Policy 935.01, Information Security Management Process.

g. Information System Access Control Review and Documentation. Facility CIOs/designees, taking into consideration each system's Risk Analysis Sensitivity Score, must approve the design and implementation of controls to limit unauthorized access of workforce members to information systems including workstations, servers, networks, and applications.

   DHS facility System Managers/Owners must document the implementation of the above safeguards in the System Security Implementation Plan that accompanies the electronic data system. The System Security Implementation Plan and all system documentation must be submitted to the DISO or designee for review.

DEFINITION:

System Security Implementation Plan. The System Security Implementation Plan is part of the system compliance documentation mentioned in DHS Policy 935.01, Information Security Management Process as well as DHS Policy No. 935.19, Data Security Documentation Requirement.

AUTHORITY:

45 Code of Federal Regulations, Part 164, Subpart C, Section 164.308 (a)(3)(ii)

CROSS REFERENCES:

DHS Policies:
- 935.01, Security Management Process: Risk Management
- 935.07, Facility Information Technology (IT) Contingency Plan
- 935.15, System Audit Controls
- 935.19, Data Security Documentation Requirement

EFFECTIVE DATE: December 1, 2010

SUPERSEDES: March 1, 2005

DEPARTMENT OF HEALTH SERVICES
COUNTY OF LOS ANGELES

SUBJECT: PERSON OR ENTITY AUTHENTICATION

POLICY NO: 935.17

PURPOSE: To verify that a person or entity seeking access to Protected Health Information (PHI) and other confidential information is the one claimed.

POLICY: Each Department of Health Services (DHS) Facility CIO/designee must establish and document facility-based procedures for each of the following requirements and submit such procedures for approval to the DISO or designee.

1. A user authentication mechanism (e.g., unique user identification and password, biometric input, or a user identification smart card) must be used for all Workforce Members seeking access to any network, system, or application that contains PHI and other confidential information.

2. Two-factor authentication, in which the user provides two means of identification, one of which is typically physical (e.g., a secure ID card using a one-time code), and the other of which is typically something memorized (e.g., a secret Personal Identification Number (PIN)) is required for all systems receiving a Risk Analysis Sensitivity score of "HIGH," (DHS Policy No. 935.01, Security Management Process: Risk Management), and for all remote access.

Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.

Users are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.

DHS Facility CIOs/designees must ensure that users make a reasonable effort to verify the identity of the receiving person or entity prior to transmitting PHI and other confidential information.

DHS Facility CIOs/designees must ensure that the DHS facility System Managers/Owners implement the system authentication mechanism that is appropriate for the risk expected for the system. System Managers/Owners must document the selected system authentication mechanism in the System Security Documentation (DHS Policy No.

935.14, System Access Control) that accompanies the electronic data system.

DEFINITION: **Authentication** means validation of the identity of the user.

For a complete definition of terms used in this policy/procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

AUTHORITY: 45 Code of Federal Regulations, Part 164, Subpart C, Section 164.312(d).
Board of Supervisor Policy Nos.:
- 6.100, Information Technology and Security Policy
- 6.101, Use of County Information Technology Resources

CROSS REFERENCES: DHS Policies:
- 361.24, Safeguards for Protected Health Information (PHI)
- 935.01, Security Management Process: Risk Management
- 935.03, Workforce Security
- 935.04, Information Access Management
- 935.14, System Access Control
- 935.20, Acceptable Use Policy for County Information Technology Resources

Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY RESOURCES

POLICY NO: 935.20

PURPOSE:

To ensure the entire Department of Health Services (DHS) workforce follow acceptable use of County information technology resources within the department.

POLICY:

Each DHS 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 DHS Policy No. 361.1, DHS Privacy and Security Compliance Program, the County Fiscal Manual, and other County and DHS information technology use policies and procedures.

All workforce members are required to sign acknowledgment of the receipt and review of the County and DHS' Acceptable Use policy (as noted below). DHS 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 "DHS Comprehensive Policy Statement" in accordance with the non-County workforce member in-processing procedures. The "DHS Comprehensive Policy Statement" must also be provided to and acknowledged by the non-County workforce member in conjunction with their annual performance review process.

APPROVED BY:
REVIEW DATES: 4/14/12

EFFECTIVE DATE: August 15, 2012
SUPERSEDES: September 1, 2009

SUBJECT: ACCEPTABLE USE OF COUNTY INFORMATION TECHNOLOGY RESOURCES

POLICY NO.: 935.20

DHS System Managers/Owners 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 DHS' County 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 DHS 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 "DHS 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 "DHS 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 DHS "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 DHS may log, review, or monitor any data created, stored, accessed, sent, or received. DHS 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 DHS network; and/or monitor sites visited on the DHS 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. DHS 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 DHS system resources is suspected. If evidence of misuse of DHS system resources is identified, the supervisor/manager must contact the DHS Audit & Compliance Division to determine appropriate actions. The DHS 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 DHS' 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 DHS or other systems.
15. Using unauthorized wired or wireless connections to DHS 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 DHS 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 DHS 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 DHS 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.

DHS 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 DHS network resources unless explicitly authorized by the Departmental Information Security Officer (DISO) or designee.

Each workforce member 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 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 DHS 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 DHS management.

Default E-Mail Retention Period

DHS 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. DHS 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 DHS 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 five or seven 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 CEO's and Executive Management from defined groups will determine which individuals will be allowed a five or seven year retention period.
d. No Personal Storage Table, (PST) files will be allowed or used by DHS 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 DHS and County Internet and privacy policies.

All DHS Internet activities are monitored and audited by DHS 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.

DHS 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 DHS shall not be liable for inadvertent exposure to any offensive materials.

Internet access is provided to the workforce member at the discretion of each DHS Facility.

VIII. INFORMATION TECHNOLOGY USER ACCOUNT MANAGEMENT

When a workforce member leaves the County service, the supervisor must inform the local service desk to have the workforce member's Information Technology (IT) user accounts deactivated immediately. All IT accounts that have been deactivated for 60 days or more will be deleted. The workforce member's supervisor will be

contacted for approval to delete the accounts. In cases where the supervisor failed to inform the local service desk, Human Resources records will be used to disable accounts that have not been active in the last 60 days. All IT accounts that have been inactive for 60 days or more will be deleted.

Each Facility's Information Technology Department shall adhere to this minimum standard/guideline.

Each Facility's 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 DHS Policy No. 935.11, Workstation Use and Security : Access and Use of Mobile Devices and DHS 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 DHS network 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 DHS network must utilize the approved DHS Information Security method for remote access. VPN is the DHS approved remote access solution 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.

WORKFORCE MEMBER Employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DHS, is under its direct control, whether or not they receive compensation from the County.

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.

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 DHS network (e.g. home) to the DHS network 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 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 Policy Nos.:
- 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

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.

Initial _____

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.**

12. 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) wrongfully 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.

Initial _____

(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 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.

ACKNOWLEDGMENT:

I acknowledge that I have received and read the Department of Health Services' Policy No. 935.20, DHS 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 or release from assignment.

If I have any questions concerning the policy or agreement, I will discuss them with my supervisor.

Name (print):	Employee/Contractor ID No.:	Date:
Signature:	Job Title:	Department No.:
Supervisor Name (print)	Supervisor Signature:	Date:

DHS Policy No. 935.20 Rev 7/6/12

Initial _____