COUNTY OF LOS ANGELES
Public Health

COUNTY OF LOS ANGELES • DEPARTMENT OF PUBLIC HEALTH

HUMAN RESOURCES

AGREEMENT OF UNDERSTANDING ▪ NON-COUNTY WORKER

NON-COUNTY WORKER NAME: (Please PRINT Last, First)	WOC#:
POSITION TITLE:	PROGRAM NAME:

DPH POLICY/ GUIDELINES	TITLE	NC WORKER INITIALS / DATE	
113	Elder/Dependant Adult Abuse		
325	Hand Hygiene in Healthcare Settings		
340	Confidentiality of Non-Patient Public Health Records		
DHS 361.23	Safeguards for Protected Health Information (PHI)		
701	Possession of a License or Certificate		
704	Professional Appearance in the Workplace		
714	Identification Badges		
722	Nepotism		
723	Designation of Sensitive Positions and Requirements for Criminal History Information		
728	Capping		
729	Political Activity		
746	Threat Management "Zero Tolerance" Policy		
748	Diversity Policy		
DHR 812	County Policy of Equity		
1000	Public Health Information Technology and Security Policy		
1016	Acceptable Use Policy for County Information Technology Resources		
1103	Exclusion of Individual/Entities from Federal Health Care Programs		
	Acceptance of Gifts Prohibitions		
	Notice of Child Abuse, Elder/Dependent Adult Abuse, Domestic/Intimate Partner Violence Reporting		
	County of Los Angeles Volunteer Workers: Indemnification & Insurance Program Description		
	Employee Safety Handbook		

I acknowledge that I have read and reviewed the listed policies/guidelines and will comply with them in my work environment. I understand that if at any time during my service as a non-County worker I have questions or concerns regarding these policies/guidelines, they shall be directed to my County supervisor or to the DPH Human Resources Office. I am aware that if I violate the above policies/guidelines I will be subject to release from service.

Non-County Worker Signature: _____ Date: _____

Reviewed by: _____ Date: _____
(DPH Program/Division Manager)

Orig: HR File
Copy: Non-County Worker

Rev. 02/2014

COUNTY OF LOS ANGELES
Public Health

SUBJECT: ELDER/DEPENDENT ADULT ABUSE	PAGE 1
	OF 2

POLICY No.: 113	EFFECTIVE DATE: 4/15/09
APPROVED BY: J E Fielding	SUPERSEDES: DHS Policy No. 295

PURPOSE: To state the Department's policy for reporting elder/dependent adult abuse.

POLICY: All Department of Public Health (DPH) employees have the responsibility to participate in identifying and reporting cases of suspect elder/dependent adult abuse. Health care professionals, including medical and non-medical practitioners, shall report all cases of suspect elder/dependent adult abuse as required by law.

Liaison with Adult Protective Services, DPSS, shall be maintained by the DPH.

GUIDE:

Identification

DPH is responsible for the identification of suspected elder/dependent adult abuse for all persons who present to its facilities. Adult abuse is defined as any act of omission or commission that endangers or impairs a person's physical or emotional health. This includes physical abuse, mental suffering, physical neglect, medical neglect, abandonment, inadequate supervision and sexual assault.

Reporting

Health Care professionals shall report suspected elder/dependent adult abuse to the appropriate agencies designated to receive such reports by telephone immediately and in writing within 36 hours of making the observation.

The agency designated to receive such reports is the Adult Protective Services Office of the Department of Public Social Services. The report shall include identifying information which will enable the Department of Public Social Services to make an evaluation of the report.

Statement of Knowledge

All new employees shall be asked to sign a dependent adult abuse reporting statement. For those persons covered by the reporting law, execution of the statement is a condition of and pre-requisite to employment with the Department. Current Public Health employees will be made aware of the reporting requirements at the time of the annual performance evaluation.

Treatment and Medical Follow-Up

Department facilities shall provide first aid, as necessary, and refer the individual to a facility for treatment that will ensure the adult's physical well-being.

AUTHORITY: Chapter 1273, Statutes of 1983 and Chapters 1120 and 1164, Status of 1985. Section 9380 through 9386 and Sections 15610, 15620 and 5621 of California Welfare and Institutions Code.

COUNTY OF LOS ANGELES
Public Health

SUBJECT: HAND HYGIENE IN HEALTHCARE SETTINGS	**PAGE** 1 OF 2
POLICY No.: 325	**EFFECTIVE DATE:** 04/30/09
APPROVED BY: Jonathan E Fielding MD	**SUPERSEDES:** DHS Policy No. 392.3

PURPOSE: To promote hand hygiene practices that reduce the transmission of pathogenic organisms to patients and personnel in health care settings.

SCOPE: This policy applies to all healthcare workers who provide direct patient care, have contact with patient care supplies, equipment or food, and laboratory and select pharmacy staff.

POLICY: It is the goal of the Department of Public Health to provide a safe and healthy environment for the treatment of patients. A major part of this goal is to promote hand hygiene and optimal hand conditions.

The following practices promote a safe environment for patients and health care workers and are to be adhered to by all health care personnel as noted in the Scope of this policy:

- Handwashing with water and plain or antimicrobial soap, or decontaminating hands with an antimicrobial agent is to be practiced as necessary and in the manner required by infection control guidelines and policies.

- Direct patient care staff and health care workers who have contact with patient supplies, equipment and food are prohibited from wearing artificial fingernails and long natural fingernails. Natural nails must be clean, with tips less than 1/4 inch beyond the tip of the finger. If fingernail polish is worn, it must be in good condition, free of chips, and preferably clear in color.

- Wearing rings with stones on fingers is discouraged. They can harbor bacteria and also tear gloves. Wearing bands may be allowed if they are cleaned along with the appropriate handwashing technique.

RESPONSIBILITY FOR COMPLIANCE: AREA HEALTH OFFICERS/DIRECTORS AND MANAGERS

1. Facility infection control managers and facility operations managers are responsible for developing internal operational procedures applicable to their facility describing proper hand hygiene protocols and infection control procedures, consistent with this policy, and CDC requirements.

2. Hand hygiene products including plain soap and/or antimicrobial soap and hand disinfecting agents (alcohol-based hand rub intended for hospital use) are to be provided in direct and indirect patient care areas. Store alcohol products in accordance with Los Angeles County regulations and National Fire Protection Agency recommendations.

3. The facility/program manager or designee is responsible for monitoring compliance with this hand hygiene policy.

4. Education regarding hand hygiene shall be provided to all employees upon implementation of this policy. This policy shall be included in the new employee orientation for health care workers as defined in the Scope of this policy.

RESPONSIBILITY FOR COMPLIANCE: EMPLOYEES

1. Employees are expected to adhere to facility policies and guidelines. Compliance with safety and infection control and prevention policies will be considered during the employee's overall performance evaluation.

2. An employee who does not comply with the fingernail provisions of this policy will be sent home without pay and not permitted to return to work until he or she has complied. Failure to comply with these requirements within 15 calendar days of being sent home may subject the employee to disciplinary action, up to and including discharge.

3. Employees are required to sign an acknowledgment that they have received a copy of this policy and agree to abide by its provisions.

DEFINITIONS:

Hand Hygiene
A general term used to describe handwashing and other methods to sanitize/decontaminate hands and proper hand care conditioning.

Artificial Fingernails
Any material applied to the fingernail for the purpose of strengthening or lengthening nails (e.g., tips, acrylic, porcelain, silk, jewelry, overlays, wraps, fillers, superglue, any appliqués other than those made of nail polish, nail-piercing jewelry of any kind, etc.)

REFERENCES: CDC Morbidity and Mortality Weekly Report, October 25, 2002, Vol. 51, No. RR-16, "Guideline for Hand Hygiene in Health-Care Settings"

COUNTY OF LOS ANGELES
Public Health

SUBJECT:	CONFIDENTIALITY OF NON-PATIENT PUBLIC HEALTH RECORDS	PAGE 1 OF 2
POLICY No.: 340		EFFECTIVE DATE: 04/30/09
APPROVED BY: Jonathan E. Freedy M		SUPERSEDES: DHS Policy No. 364

PURPOSE: To state the Department's position regarding confidentiality of non-patient public health records.

POLICY: Certain records maintained by the Department are public records.

Matters considered to be public records include:

1. Environmental Health official inspection reports (excluding complaints).
2. Environmental Health prosecution reports at termination of litigation.
3. The following Health Facilities Division records: license applications, current licenses, inspection reports and plans for correction.
4. Acute Communicable Disease Control outbreak summary reports.
5. Public Health Investigation Commercial Sex Venue Official Inspection Reports.
6. Informational certified copies of birth and death certificates maintained in Vital Records.
7. Animal bite reports (excluding personal and medical information pertaining to the bite victim).

GUIDE: All other departmental records shall be considered confidential and may be released only when directed by a court, through court order or an appropriately executed Subpoena Duces Tecum served on the designated Custodian of Records, or with the written consent of the individual to whom the information pertains or their legal representative.

The Custodian of Records shall answer inquiries and shall be provided statements to be used in court appearances by County Counsel.

AUTHORITY: California Government Code
California Health and Safety Code
California Evidence Code
California Code of Regulations, Titles 17 and 22

County Counsel written opinion relating to confidentiality of information contained in animal bite reports.

DEPARTMENT OF HEALTH SERVICES
COUNTY OF LOS ANGELES

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI)

POLICY NO: 361.23

PURPOSE:

To establish safeguards that must be implemented by DHS to protect the confidentiality of protected health information.

POLICY:

Set forth below are policies establishing minimum administrative and physical standards regarding the protection of protected health information that DHS must enforce. DHS may develop additional policies and procedures that are stricter than the parameters set forth below in order to maximize the protection of protected health information in support of their specific circumstances and requirements. The development and implementation of policies and procedures in addition to those stated herein must be approved by the Chief Information Privacy Officer.

DHS will implement appropriate administrative, technical, and physical safeguards which will reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of DHS' Privacy Policies.

DHS' Workforce must reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

DEFINITIONS:

Protected Health Information (PHI) means individually identifiable information relating to past, present or 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.

Particularly Sensitive Health Information means protected health information that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse, and communicable disease information.

Workforce or Workforce Member means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DHS, is under its direct control, whether or not they are paid by the County.

PROCEDURES:

A. Administrative Safeguards.

1) Oral Communications. DHS' Workforce must exercise due care to avoid unnecessary disclosures of protected health information through oral communications. Conversations in public areas should be avoided, unless necessary to further patient care, research or teaching purposes. Voices should be modulated and attention should be paid to unauthorized listeners in order to avoid unnecessary disclosures of protected health information. Patient identifying information only should be disclosed during oral conversations when necessary to further treatment, payment, teaching, research or operational purposes. Dictation and telephone conversations should be conducted away from public areas if possible. Speakerphones only should be used in private areas.

2) Cellular Telephones. The use of cellular phones is not prohibited as a means of disclosing or using PHI. However, their use poses a higher risk of interception as compared to legacy landline telephones. Landline telephones should be used if the conversation will involve the disclosure of PHI.

3) Telephone Messages. Telephone messages and appointment reminders may be left on answering machines and voice mail systems, unless the patient has requested an alternative means of communication pursuant to **DHS Policy No. 361.6, "Right to Request Confidential Communications of Protected Health Information."** However, each provider and/or clinic should limit the amount of protected health information that is disclosed in a telephone message. The content of appointment reminders should not reveal Particularly Sensitive Health Information, directly or indirectly. Telephone messages regarding test results or that contain information that links a patient's name to a particular medical condition should be avoided.

4) Faxes. The following procedures must be followed when faxing PHI:

a) Only the PHI necessary to meet the requester's needs should be faxed.

b) Particularly Sensitive Health Information should not be transmitted by fax, except in emergency situations or if required by a government agency. If Particularly Sensitive Health Information must be faxed, the recipient should be notified immediately prior to the transmission and the sender should immediately confirm that the transmission was completed, if possible.

c) DHS should designate employees who can fax, or approve the faxing of, protected health information. Unauthorized employees, students and volunteers should never fax protected health information.

d) Unless otherwise permitted or required by law, a properly completed and signed authorization must be obtained before releasing protected health information to third parties for purposes other than treatment, payment or health care operations as provided in **DHS Policy No. 361.4, "Use and Disclosure of Protected Health Information Requiring Authorization."** Protected health information may be faxed to an individual if the individual requests access to their own protected health information in accordance with **DHS Policy No. 361.15, "Access of Individuals to Protected Health Information (PHI)/Designated Record Set."**

e) All faxes containing protected health information must be accompanied by a cover sheet that includes a confidentiality notice. Use DHS' ***PHI FAX Form***.

f) Reasonable efforts should be made to ensure that fax transmissions are sent to the correct destination. Frequently used numbers should be preprogrammed into fax machines or computers to avoid misdialing errors. Preprogrammed numbers should be verified on a routine basis. The numbers of new recipients should be verified prior to transmission.

g) Fax machines must be located in secure areas not readily accessible to visitors and patients. Incoming faxes containing protected health information should not be left sitting on or near the machine.

h) Fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet should be attached to the document that was faxed.

i) All instances of misdirected faxes containing protected health information should be investigated and mitigated pursuant to **DHS Policy No. 361.26, "Mitigation."**

5) Mail. Protected health information should be mailed within the County's departments in sealed envelopes. Protected health information mailed outside the County's departments should go via first class mail and should be concealed. Appointment reminders may be mailed to patients, unless the patient has requested an alternative means of communication pursuant to **DHS Policy No. 361.6, "Right to Request Confidential Communications of Protected Health Information."**

6) Destruction Standards. Protected health information must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing protected health information should be destroyed or shredded. Magnetic media and diskettes containing protected health information should be overwritten or reformatted.

   a) PHI awaiting disposal must be stored in containers that are appropriately labeled and are properly disposed of on a regular basis.

   b) Storage rooms containing confidential information awaiting disposal must be locked after business hours or when authorized staff are not present.

   c) Centralized bins or containers used for disposed confidential information must be sealed, clearly labeled "confidential", "PHI" or some other suitable term and placed in a locked storage room.

   d) Facilities or sites that do not have protected storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to PHI.

B. Physical Safeguards.

1) Paper Records. Paper records and medical charts must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier should be used to protect paper records from unauthorized access.

   a) Paper records and medical charts on desks, counters or nurses stations must be placed face down or concealed to avoid access by unauthorized persons.

   b) Paper records should be secured when the office is unattended by persons authorized to have access to paper records.

   c) Original paper records and medical charts should not be removed from the premises unless necessary to provide care or treatment to a patient or required by law.

      i. DHS employees should not remove paper records or medical charts for their own convenience.

      ii. Any paper records and medical charts removed from DHS' premises should be checked out according to DHS' policies and procedures and should be returned as quickly as possible.

iii. The safety and return of the medical records checked out or removed are the sole responsibility of the person who checked them out or removed them.

iv. Paper records and medical charts that are removed from DHS' premises must not be left unattended in places in which unauthorized persons can gain access.

v. Paper records and medical charts must not be left in unlocked automobiles or in view of passers-by.

vi. The theft or loss of any paper record or medical chart should be reported to the DHS' Privacy Officer so that mitigation options can be considered.

C. Physical Access

1) Persons authorized to enter areas where PHI is stored or viewed must wear identifiable, DHS employee badges or be escorted by an authorized County employee.

2) Persons attempting to enter an area where PHI is processed must have prior authorization by DHS management.

3) Employees must not allow others to use or share their badges and must verify access authorization for unknown people entering an area where PHI is stored or processed.

4) Terminated or transferred personnel must be escorted in areas where PHI is stored or processed.

D. Escorting Visitors and Patients.

Visitors and patients must be appropriately monitored when on DHS' premises where protected health information is located to ensure they do not access protected health information about other patients without permission. This means that persons who are not part of DHS' Workforce should not be in areas in which patients are being seen or treated or where PHI is stored without appropriate supervision.

E. Computer/Work Stations.

Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation. Suggested means for ensuring this protection include:

1) Use of polarized screens or other computer screen overlay devices that shield information on the screen;

2) Placement of computers out of the visual range of persons other than the authorized user;

3) Clearing information from the screen when not actually being used;

4) Using password protected screen savers when computer workstations are not in use.

F. Technical Safeguards.

1) Technical safeguards regarding the protection of Protected Health Information maintained in electronic form may include:
   - Log off any electronic system containing PHI when leaving the computer or after obtaining necessary data
   - Do not share computer passwords or leave them out where they can be seen.
   - Change passwords every three (3) months.
   - Ensure all computers and laptops used to access PHI are properly secured.
   - Become familiar with departmental contingency plan.
   - Ensure that all areas used to store PHI are properly secured and that only authorized personnel have access to these locations.

2) Use of Electronic Systems. Until appropriate security mechanisms are implemented and supporting policies are published, DHS' Workforce will not be permitted to use the following electronic systems for the distribution, processing or storage of PHI:

   a) Electronic mail or email;

   b) Personal Digital Assistance (PDA), such as Palm Pilot, iPAQ, Window's CE or other similar devices.

c) Wireless networks

G. Document Retention. This policy will be retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

REFERENCES

Code of Federal Regulations 45 § 164.530 (c) (1)
DHS Policy Nos. 361.6, "Right to Request Confidential Communications of Protected Health Information"
361.15, "Access of Individuals to Protected Health Information (PHI)/Designated Record Set"
361.26, "Mitigation"

COUNTY OF LOS ANGELES
Public Health

SUBJECT: POSSESSION OF A LICENSE OR CERTIFICATE	PAGE 1
	OF 2

POLICY No.: 701	EFFECTIVE DATE: 09/30/09
APPROVED BY:	SUPERSEDES: DHS Policy No. 704

PURPOSE: To establish that it is the employee's responsibility for presenting and maintaining a current license and/or certificate that is a requirement of his/her classification.

POLICY: Any employee who is being placed in a classification which requires a current valid license or certificate to perform the duties of this classification will produce evidence of this licensure or certification to the Department of Public Health (DPH) Human Resources office prior to being placed on this classification. After placement, it will also be the employee's responsibility to maintain all required licenses and certificates are kept current.

TEMPORARY POSITIONS

Persons recruited for positions requiring licensure or certification may be appointed to a temporary position pending receipt of such license or certificate. This shall not apply to medical, dental, and other professionals where such action would constitute a breach of the Business and Professions Code.

Any persons so employed shall be notified in writing of the conditions of employment by the appointing authority at the time of appointment. This notification shall also include the date by which the employee must obtain the required license/certificate. If the employee fails to obtain the required license/certificate by the due date, the employee will be released from County service or demoted, as applicable.

MAINTAINING CURRENT LICENSE/CERTIFICATE

Any employee whose classification requires a current valid license or certificate to perform the duties of his/her classification and who fails to renew or maintain a current valid license or certificate, will be subject to disciplinary action in accordance the Department's Employee Evaluation and Discipline Guidelines (EE&DG).

Where applicable, licenses and/or certificates are subject to verification by Department management via the Primary Source Verification process.

GUIDELINES:

The Director of the Department's Human Resources shall establish procedures to ensure that employees are aware of this policy. Such procedures shall include, but are not limited to, the following:

1. Review of this policy with each incoming employee and document said review in the personnel file.

2. Review of this policy by supervisor/manager and the employee at the time of the annual Performance Evaluation, in accordance with Performance Evaluation Policy.

3. Written notice provided to volunteers, contractors, and other non-compensated workers.

AUTHORITY: Civil Services Rule 18.031

COUNTY OF LOS ANGELES
Public Health

SUBJECT: PROFESSIONAL APPEARANCE IN THE WORKPLACE	PAGE 1 OF 3
POLICY No.: 704	EFFECTIVE DATE: 02/01/10
APPROVED BY: Jonathan Fielding MD	SUPERSEDES: DHS Policy No. 706.01

PURPOSE: To establish a policy for professional appearance in the workplace for the Department of Public Health (DPH) employees and to ensure compliance with County Policy, 512 Professional Appearance in the Workplace and County Code Section 5.72.010.

POLICY: DPH employees are required to wear clothing suitable to their occupations, as may be determined by the Director of Department of Public Health. Employees shall furnish and maintain in suitable and appropriate condition such clothing and associated articles at their own expense except as otherwise expressly provided for by the Board of Supervisors. Employees should maintain a neat and professional appearance in the performance of their duties.

GUIDELINES:

DPH provides a wide variety of programs and services and the professional image of our workforce is critical to fostering public confidence and providing "effective and caring service." Therefore, these guidelines on professional appearance are intended to:

- Foster respect and earn the confidence of our customers, the public, vendors and fellow employees.
- Promote a positive work environment and limit distractions.
- Ensure safety and security while working.

DPH respects the diversity of its residents and its workforce. This policy provides guidelines on dress and appearance appropriate to the nature of the work environment, nature of work performed, involvement with the service provided to the public, and/or other circumstances or business needs as defined by the Director of Public Health.

Employees are expected to abide by the following standards:

- Employees shall present a neat, clean, and professional appearance in their performance of duties at all times based on the employee's assignment and/or work location.
- Employees must dress in a manner that will not hinder their ability to effectively complete their work assignments, including consideration of the communities served, customer expectations, business needs or standards of the department and the employee's safety.
- Employees are expected to practice personal hygiene that does not interfere with the public and/or co-workers in their work environment.
- Employees should be mindful of, and dress appropriately for, special events, meetings and appointments with customers.
- Official photo identification badges and uniforms (where applicable) should be worn in the performance of County of Los Angeles business and in all County of Los Angeles facilities in order to identify employees as legitimate County representatives.
- Employees shall abide by specific dress requirements intended to ensure job-related safety such as when operating equipment or machinery, working with potentially dangerous chemicals, or for public health consideration.

Except as noted or approved by the Director of Public Health, DPH employees may not wear the following:

- T-shirts or clothing articles that may create a hostile or abusive work environment, such as sexually suggestive cartoons, pictures, or words.
- Denim pants or jean-style pants of any color except for carpenter and ground maintenance worker assignments which include carpet laying, moving equipment, and repairing and assembling equipment.
- Pants below the waistline or low-rise pants showing undergarments.
- Low front tops, halter tops, bare midriffs.
- Flip-flop styled sandals.
- Athletic wear, e.g., gym or sweat pants, leggings, jogging outfits, shorts, spandex, worn during work hours. Exception for break time when walking, running, etc.
- Torn, frayed, or ripped clothing.
- Excessively tight fitting or oversized (baggy) garments.
- Visible excessive number of earrings and/or studs; no nose, eyebrow, lips, tongue rings and/or studs.
- Tattoos, must be reasonably covered (with exception for cultural or religious purposes).

Exceptions to this policy may be made by the Director of Public Health in circumstances such as County of Los Angeles or DPH-sponsored events, special occasions, seasonal weather changes, and business casual days, but may also be made based on the requests for reasonable accommodation (e.g., religious, cultural, disability, etc.).

Dress Policy Enforcement

This policy is intended to provide guidelines on dress and appearance and is not meant to address all situations. Therefore, depending on the nature of the work environment, nature of work performed, involvement with the public, or other circumstances, there may be some differences in dress guidelines. Consistent with this policy, exceptions can be made at the department level by the Director of Public Health with approval from the Director of Human Resources due to the nature of work, special events, and business casual days. Employees who report to work and are not in compliance with this policy may be sent home to change and return to work, unless some other remedy can be arranged, such as an employee putting on a jacket.

Any questions regarding the dress policy within your department should be directed to the DPH Human Resources Office.

AUTHORITY: County Code, Title V Personnel, Section 5.72.010 – Suitable clothing to be worn.

Department of Human Resources Policy Number 512

County of Los Angeles Employee Handbook, Section C, Performance Expectations

COUNTY OF LOS ANGELES
Public Health

SUBJECT: IDENTIFICATION BADGES	PAGE 1 OF 3
POLICY No.: 714	EFFECTIVE DATE: 01/31/10
APPROVED BY:	SUPERSEDES: DHS Policy No. 940

PURPOSE: To assure proper identification for all personnel working in the Department of Public Health (DPH).

DEFINITION:

Personnel is defined as employees, duly authorized contractors, student, agency personnel, and volunteer, whether they are permanent, temporary, or part-time.

POLICY: Department of Human Resources shall control the issuance and the return of official identification badges to all personnel. It is the responsibility of personnel issued identification badges to wear them in a prominently displayed position at all times while on County premises.

All identification badges shall contain the County Seal or graphic and designate the Department by which the employee is employed. The badge shall contain the following identifier information:

a) A recent photograph of the individual (within the last five years);
b) The full name of the individual, his/her employee number or agency number, and Department title or agency title;
c) Signature of the individual and/or the appointing authority;
d) The individual's birth date, height, eye and hair color.

Badges shall be approximately 3½ inches wide by 2½ inches high. Badges must be laminated securely, both front and back.

IDENTIFICATION BADGE REPLACMENT PROCEDURES

It is the individual's responsibility to report the loss or theft of the identification badge within five business days to the law enforcement agency having jurisdiction over the location where the incident occurred.

Each individual must sign an affidavit attesting to the fact that the identification badge was lost or stolen.

Each individual will be required to pay for the replacement cost of his/her identification badge if it is not returned, lost, damaged, or destroyed due to personal negligence.

Therefore, prior to the issuance of a duplicate identification badge, the individual must provide a copy of a police or Office of Security Management (OSM) report, complete and sign an affidavit, provide a check or money order for the replacement of the identification badge, and present the items to the Department Human Resources office.

Copies of the affidavit and police or OSM report will be filed in the individual's official personnel/agency file.

The replacement fee for lost or stolen identification badges is as follows:

First identification badge replacement:	$25.00
Second identification badge replacement:	$50.00
All subsequent identification badge replacement:	$100.00

TRANSFER TO OTHER COUNTY DEPARTMENTS

When an individual transfers to another facility or leaves the department, it is his/her responsibility to return his/her badge to his/her supervisor. If the badge is not returned, Human Resources staff will not process the transfer documents until such time as the identification badge is returned or a copy of the police or OSM report, affidavit and replacement cost is submitted to the Department of Human Resources.

TERMINATIONS

When an individual terminates County service, it is his/her responsibility to return his/her badge to his/her supervisor. If the badge is not returned, the individual must submit a copy of the police or OSM report along with the affidavit.

If a compensated paid individual such as an employee or contractor, does not submit either the badge or the copy of the police or OSM report and affidavit, the payment of his/her accrued benefits will be withheld up to three months.

If a compensated paid individual such as an employee or contractor, states that he/she has the identification badge but refuses to return it, the payment of his/her accrued benefits will not be issued until such time as the identification badge is submitted. Additionally, if a compensated paid individual, such as an employee or contractor, does not return the identification badge, DPH Human Resources will report the non return of the identification badge to OSM via a Security Incident Report, within 24 hours of being notified the identification badge has not been returned.

NON COMPLIANCE

Failure to comply with the provisions of this policy will result in disciplinary action in accordance with the DPH Employee Evaluation and Discipline Guidelines.

AUHTORITY: County Code Section 5.64.180
County Code Section 5.64.190
County Code Section 5.64.330
County Code Section 5.64.340
County Code Section 5.64.040

ACKNOWLEDGMENT

By my signing where indicated below, I acknowledge that I have received and reviewed a copy of the Department of Public Health Identification Badge policy.

Name (Print):	**Employee Number:**	**Date:**
Signature:	**Job Title:**	
Supervisor Name (Print):	**Supervisor Signature:**	**Date:**

Distribution:

Employees:

Original: Employee Official Personnel Folder
Copy: Employee, contractor, volunteer, or student

COUNTY OF LOS ANGELES
Public Health

SUBJECT: NEPOTISM	**PAGE** 1 of 3
POLICY No.: 722	**EFFECTIVE DATE:** 01/31/10 **REVISED:** 11/30/11
APPROVED BY: Jonathan E. Fielding MD	**SUPERSEDES:** DHS Policy No. 708

PURPOSE: To ensure the integrity of employment decisions and of the overall operations of the Department, with the objective of preventing favoritism or preferential treatment arising out of the actual or perceived conflicts of interest (involving, among other things, direct supervision of relatives, personal relationships), fraud and other abuses.

POLICY: Immediate relatives shall not be assigned within the same budgetary/organizational unit. A workforce member may not supervise a relative, either as an immediate supervisor or as a higher-level supervisor, except as provided for in this policy.

An individual shall not be assigned to a position under the direct or indirect supervision or control of an immediate relative who has or may have a direct effect on the individual's assignment, progress, performance or advancement.

Managers and supervisors should also evaluate any potentially sensitive situations involving personal relationships within their area(s) of responsibility. Although it is unlawful to discriminate on the basis of marital status or personal relationships, managers/supervisors may reasonably regulate the work situation of individuals in relationships as defined in this policy to ensure fair and impartial treatment of employees relative to employment decisions, safety, security, and/or morale.

Each workforce member shall be responsible for reporting any relationships he/she may have that may be governed by the provisions of this policy, including personal relationships (as defined herein).

DEFINITIONS:

1. **Budgetary/organizational unit** means the divisions, programs and units within the DPH reporting structure as established by the Department and the Chief Executive Office.

2 **Immediate relative** includes any relationship formed by blood, genealogy, marriage, adoption, cohabitation, and domestic partnership as defined in California Family Code Section 297 et seq. and Los Angeles County Code Section 2.210, including but not limited to spouse (common laws or otherwise), child, mother , father, sister, brother,

aunt, uncle, grandparent, niece, nephew, step-parent, step-child, step-sibling, cousin or legal guardian.

3. **Nepotism** is generally defined as the practice of a workforce member using personal influence or power to aid an immediate family member in an employment setting in securing employment, promotion or other benefits.

4. **Personal relationships** include, but are not limited to, those by virtue of blood, marriage, adoption, cohabitation, committed, or any such personal relationship which would give rise to a substantial appearance of impropriety or lack of reasonable objectiveness if the person were to be supervised as set forth in this policy.

5. **Workforce members** include employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DPH, is under its direct control, whether or not they receive compensation from the County.

· GUIDELINES:

At the time a person is processed in for a position in DPH and on an annual basis thereafter, he/she must identify any person employed by DPH with whom they have a relationship as designated above.

The Director, DPH Human Resources shall establish procedures to ensure that employees are aware of the policy. Such procedures shall include, but not be limited to, the following:

1. A review of this policy with each incoming employee and documented in the personnel file.

2. Supervisors/managers will also review this policy with employees at the time of the employee's annual performance evaluation, and this review will be documented in the employee's personnel file.

The employee must immediately notify his/her supervisor if a situation arises, either as a result of a new-hire, transfer-in, promotion, reorganization and/or marriage, in which immediate relatives or a personal relationship exists (as defined above) are employed within the same budgetary organizational unit or are supervised by the same individual. The appropriate Program Manager may request one of the individuals to transfer to a similar item in a different budgetary organizational unit of the Department.

EXCEPTIONS:

In some instances, a situation may technically violate the Department's policy but not present a conflict of interest and therefore may warrant an exception.

In evaluating a request for an exception to the policy, the overall objectives of the policy should be weighed against the reason for requesting an exception, on a case-by-case basis.

PROCEDURES FOR REQUESTING EXCEPTIONS:

If a manager/supervisor determines that a request for an exception is appropriate, a memo establishing the justification for the request, an organization chart explaining the functional responsibilities of the related employees or those work force members in which a personal relationship exists, and a statement of why it is believed problems will not result, shall be forwarded through the chain-of-command to the appropriate Program Manager.

All requests for exceptions must be submitted to the appropriate Executive Manager, and if approved by the Executive Manager, forwarded to the Department of Public Health Audit and Compliance Unit for review and final approval.

COUNTY OF LOS ANGELES
Public Health

SUBJECT: DESIGNATION OF SENSITIVE POSITIONS AND REQUIREMENTS FOR CRIMINAL HISTORY INFORMATION	PAGE 1 OF 7

POLICY No.: 723	EFFECTIVE DATE: 09/30/09 **REVISED DATE: 01/30/11**
APPROVED BY: Jonathan E. Fielding, M.D.	**SUPERSEDES:** DHS Policy No. 703.1

PURPOSE: To provide guidelines to implement the Board of Supervisors adopted Resolution regarding access of criminal history information in connection with employment in sensitive positions.

To ensure that any person hired, promoted, or transferred to another position obtains work clearance through a LiveScan fingerprint process and criminal records background check to assure that any criminal record or criminal conviction does not conflict with duties to be performed or does not pose a potential threat to the Department of Public Health (DPH) or the public served in performance of duties.

POLICY: Every position within DPH is judged to be a sensitive position, and therefore, covered by this policy and guidelines.

All newly hired employees, reinstatements, restorations, commissioners, interns, students, volunteers, and contract workers, both permanent and temporary, as well as employees who are (1) changing their items/classifications or (2) transferring or promoting from within DPH or from other County departments are covered by this policy and are to be fingerprinted. Fingerprints are submitted to the State Department of Justice for a criminal records background check. Employment is contingent upon the outcome of the background check. Certain criminal offenses may disqualify an individual from employment.

The DPH shall not place a person in a sensitive position if he/she has been convicted of a felony or misdemeanor, except that such conviction may be disregarded if it is determined that there were mitigating circumstances or that the conviction is not related to the position and poses no threat or risk to the County or the public. Each case is to be individually reviewed and evaluated by the Public Health Human Resources Director or his/her designee.

The DPH shall consider as sensitive any position involving duties which pose a threat or risk to the Department or to the public when performed by persons who have a criminal history incompatible with those duties, whether those persons are employees of the Department or perform those services pursuant to contract or a volunteer basis.

Any current workforce member **charged** with any crime (including, traffic violations, if position requires driving on County business) shall report being charged with such crime to DPH Human Resources within 72 hours of becoming aware of the charge. A current workforce member **convicted** of a crime (including a traffic violation, if the position requires driving on County business) shall report the conviction to DPH Human Resources Performance Management Unit within one working day subsequent to the conviction. Failure to report may result in disciplinary action, including discharge from the County or termination from the assignment.

GUIDELINES:

A. Mandatory Criminal History Information Request – Sensitive Positions

The Department of Public Health must secure criminal history information on selected candidates for vacant positions, contract personnel, interns, and volunteers performing duties within the following categories:

- Positions that involve the care, oversight, or protection of persons through direct contact with such persons (e.g., Public Health Nurses, Home Nursing Attendant, Clinical Social Worker, Community Workers, Clinic Driver, Licensed Vocational Nurse, etc.).
- Positions having direct or indirect access to funds or negotiable instruments, (e.g., Chief Financial Officer, Finance Manager, Revenue Manager, Deputy Purchasing Agent, Cashier, etc.).
- Positions that require state and/or professional licensing (e.g., Physician, Registered Nurse, Certified Public Accountant, Pharmacist, Physical Therapist, etc.).
- Positions that involve public safety and/or law enforcement, (e.g., Safety Police Officer, Probation Officer, Public Health Investigator, Environmental Health Specialist, Health Facilities Evaluators, etc.).
- Positions that have access to or charge for drugs or narcotics (e.g., Pharmacist, Pharmacist Technician, Pharmacy Helper, Physician, Registered Nurse, etc.).
- Positions that have access to confidential or classified information including criminal conviction information (e.g., Personnel Officer, Department Personnel Technician, Psychiatric Social Worker, etc.).
- Positions that involve the care, oversight, or protection of County, public, or private property (e.g., Estate Property Custodian, Warehouse Worker, etc.).

B. Potentially Disqualifying Job Related Offenses

The following identifies offenses which, under certain conditions, may be incompatible with specific work functions. These lists shall be used as general

guidelines in determining which criminal offenses are related to the duties of sensitive positions.

- **Function** – Care, Oversight, or Protection of Persons through Direct Contact with Such Persons. **Offense:**

  Robbery, Intoxication, Theft
  Embezzlement, Fraud, Forgery
  Kidnapping, Manslaughter, Assault
  Homicide, Elder Abuse, Child Abuse
  Receiving Stolen Property, Drug or Narcotics Offenses
  Sex Offenses which involve Victims; e.g., Rape, Child Molestation, etc.

- **Function** – Direct or Indirect Access to Funds or Negotiable Instruments. **Offense:**

  Bribery, Robbery, Theft
  Fraud, Embezzlement, Forgery
  Receiving Stolen Property

- **Function** – Requirement of State and/or Professional Licensing. **Offense:**

  Violation of any certification or licensing provisions relating to duties of the position in question may also be the basis for disqualification.

- **Function** – Public Safety or Law Enforcement. **Offense:**

  Robbery, Theft, Perjury
  Embezzlement, Kidnapping, Fraud
  Homicide, Intoxication, Assault
  Drug or Narcotics Offenses, Forgery
  Sex Offenses which involve Victims; e.g., Rape, Child Molestation, etc.

- **Function** – Access to or Charge for Drugs or Narcotics. **Offense:**

  Robbery, Fraud, Theft
  Embezzlement, Forgery
  Receiving Stolen Property, Drug or Narcotics Offenses

- **Function** – Access to Confidential or Classified Information Including Criminal Conviction Information. **Offense:**

  Extortion, Robbery, Theft
  Fraud, Forgery, Perjury
  Receiving Stolen Property

- **Function** – Charge of Access to County, Public or Private Property. **Offense:**

  Robbery, Embezzlement

Receiving Stolen Property Theft

C. Hiring Standards

Persons with criminal records may be eligible for placement in a sensitive position for which they otherwise qualify and in which their previous conviction does not pose a risk. Each case is to be individually reviewed and the evaluation should consider:

- The nature of the offense in relation to the position's duties.
- The seriousness of the offense as evidenced by conditions surrounding the crime and the sentence given. Any extenuating circumstances are to be taken into consideration.
- The recency of the offense.
- The age of the individual at the time the offense and the conviction took place.
- The extent of the individual's criminal record. Was the offense and conviction an isolated incident or does it represent a continuing pattern?
- The evidence and extent of rehabilitation by the individual.
- The subsequent period of stability (i.e., has the applicant been free from further convictions?).
- Employee's work history (e.g., performance evaluations, length of service, prior disciplinary action, commendations, etc.).
- Disclosure of convictions on Employee Information Sheet and/or applications.

PROCEDURES: The DPH Human Resources Director is designated as the custodian of information regarding criminal convictions and will be responsible for its security and confidentiality. Therefore, the DPH HR Director will ensure the following:

- All fingerprinting and criminal conviction information is maintained under lock and key and does not leave the premises of DPH HR.
- It is determined whether or not there is a legitimate "need to know" reason for any request by an individual to review DOJ information.
- A Live Scan Visitors Log is maintained that contains (1) the name and title of the individual reviewing the information; (2) the date and time the individual examined the information; (3) the "need to know" reason for viewing; (4) and the DPH HR Director's signature approving the examination of the information.
- DOJ Information is accessed by designated staff only.

- A log for all individuals to be fingerprinted is maintained that contains the following information: name, date of birth, social security number, job title/position, program name, date submitted, date results received, initial of the HR staff member performing the LIVE SCAN, Applicant Transaction Identifier (ATI) number, cleared status yes/no.

- All automated systems containing conviction information is secured to prevent unauthorized access, alteration, deletion, or release of the information.

- Live Scan Computer terminals are located in secure premises.

- Retention or sharing of conviction information by unauthorized staff is strictly prohibited.

- Criminal history information will only be used for hiring/appointing purposes and is not to be reproduced for secondary dissemination.

- All staff with access to criminal history information is certified to function as an operator and is trained and counseled on the handling of the strictly confidential criminal history information.

- For any individual who has a record of criminal arrests or convictions, a thorough review is conducted to determine if a job nexus would exist. This would include performing the following:

  - Obtaining court record information

  - Obtaining written statement from individual

  - Evaluating the conviction to the job or service being performed (see Hiring Standards above).

  - Assessing work history

- A No Longer Interested Notification Form to DOJ is submitted to discontinue receipt of subsequent report notification when employment is terminated or the applicant is not hired.

- The Job Nexus Evaluation Form is completed when a criminal record is reported by the DOJ.

LIVESCAN: All individuals who are required to be digitally fingerprinted shall be advised in writing that employment is contingent upon the outcome of the criminal records background check and that any conviction(s) disclosed in the background check may be cause for DPH not to appoint the individual.

In addition, any criminal record that is subsequently disclosed via the Live Scan and which was not disclosed on the applicant's application and/or Employee Information Sheet will subject that individual to direct disqualification, or if an employee applicant, to disciplinary action in accordance with the Department of Public Health Employee Evaluation and Discipline Guidelines.

(1) Designated DPH HR staff shall assist the individual/applicant in completing the REQUEST FOR LIVE SCAN SERVICE, Applicant Submission form (DOJ form #BCII 8016, Attachment I), accurately and clearly.

(2) Each candidate must furnish a current and valid photo identification, i.e., Driver's License, Passport, etc. The candidate will then be fingerprinted via the Live Scan terminal.

(3) The information from the Applicant Submission form is entered into the Live Scan terminal using the Live Scan Data Entry Guide, and fingerprints are then scanned.

(4) After successful entering of information and electronic capture of fingerprints, the information is electronically transmitted to the State of California Department of Justice.

(5) Upon clearance, the program office will be notified, and the final hiring or appointment process will be initiated.

Designated DPH HR staff will follow-up with the Department of Justice regarding fingerprint results that have not been returned within ten (10) working days.

Upon determination of the individual's fitness for the position, the record results shall be destroyed to the degree that the identity of the individual can no longer be reasonably ascertained.

Retention of criminal history records will be based upon documented legal authority and need. These records will be stored in a secure, confidential manner.

DPH will also receive subsequent notification from the Department of Justice if the individual has been arrested any time after his/her LIVESCAN has been processed. These notifications will be forwarded to the DPH Performance Management Unit for follow-up and corrective action.

AUTHORITY:

- California Code of Regulations, Title 11, Section 708
- Penal Code Sections 11105 (b)(10) and 13300 (b)(10)
- County Code Civil Service Rules 6.04 and 18.03

- Los Angeles County Department of Human Resources Policy #514:
- Designation of Sensitive Positions and Requirements for Criminal History Information
- November 10, 1998, Resolution of the Board of Supervisors of County of Los Angeles declaring its intention to provide for the access of criminal history information for employment in sensitive positions
- Los Angeles County Department of Human Resources Accessing & Assessing Criminal History Information Guide – 2008/2009

Criminal Offenses that may be Incompatible with Certain Work Function

Note: This is not meant to be an exhaustive list, and other offenses may result in a determination of unsuitability for employment based upon job nexus. Additionally, the list of offenses under each function is not meant to be exhaustive, and may include other offenses as well.

- Function: Care, Oversight, or Protection of Persons through Direct Contact with Such Persons:

  Robbery; Intoxication; Theft; Forgery; Embezzlement; Kidnapping; Homicide; Fraud; Manslaughter; Assault; Child Abuse; Drug or Narcotics Offenses; Elder Abuse; Receiving Stolen Property; Sex Offenses including, but not limited to: Rape, Child Molestation, etc.

- Function: Direct or Indirect Access to Funds or Negotiable Instruments:

  Bribery; Robbery; Theft; Fraud; Embezzlement; Forgery; Receiving Stolen Property;

- Function: Requirement of State and/or Professional Licensing:

  Violation of any certification or licensing provisions;

- Function: Access to or Charge of Drugs or Narcotics:

  Robbery, Fraud, Theft, Embezzlement, Forgery, Drug or Narcotics Offenses, Receiving Stolen Property;

- Function: Access to Confidential or Classified Information Including Criminal Conviction Information:

  Extortion, Robbery, Theft, Fraud, Perjury, Receiving Stolen Property;

- Function: Charge of, or Access to County Property

  Robbery, Embezzlement, Theft, Receiving Stolen Property

COUNTY OF LOS ANGELES
Public Health

SUBJECT: CAPPING	**PAGE** 1
	OF 1

POLICY No.: 728	**EFFECTIVE DATE:** 01/31/10
APPROVED BY:	**SUPERSEDES:** DHS Policy No. 743

PURPOSE: To identify Department of Public Health (DPH) enforcement of California Business and Professions Code as it relates to capping.

POLICY: DPH employees shall not engage in capping activities on or off County property. It is the responsibility of the appointing authority to require new employees to sign a statement acknowledging that they have been informed of the illegality of soliciting business for attorneys, both on and off County property.

DEFINITION: Capping is soliciting business for attorneys. A "capper" is any person, firm, association, or corporation acting in any manner, or in any capacity, as an agent for an attorney at law in the solicitation of business.

GUIDELINES: The Director, Human Resources shall establish procedures to ensure that employees are aware of the policy. Such procedures shall include, but not be limited to the following:

1. A review of this policy with each incoming employee and documented in the personnel file.

2. Supervisors/managers will also review this policy with employees at the time of the employee's annual performance evaluation, and this review will be documented in the employee's personnel file.

AUTHORITY: California Business and Professions Code, Sections 6151 and 6152.

COUNTY OF LOS ANGELES
Public Health

SUBJECT: POLITICAL ACTIVITY	PAGE 1 OF 2
POLICY No. : 729	EFFECTIVE DATE: 01/31/10
APPROVED BY: Jonathan E. Fielding, MD	SUPERSEDES: DHS Policy No. 744

PURPOSE: To establish policy governing the political activities of the Department of Public Health (DPH) employees.

POLICY: DPH employees shall refrain from political activities while in their official capacity. While it is essential that County employees be free to exercise their rights and privileges as citizens, their position in government often gives greater influence to their actions than to similar actions by other citizens. In fact, actions which may be proper for an ordinary citizen may be improper and unethical for a County employee.

A County employee who engages in the following improper activities shall be subject to immediate disciplinary action:

1. Knowingly soliciting or receiving political funds or contributions from County employees or from persons on County eligible lists.

   EXCEPTION: Soliciting funds for passage or defeat of a ballot measure affecting the pay, hours, retirement, and service or other working conditions of County employees is permitted in off duty hours.

2. Participating in political activities which conflict with, limit, or restrict the daily effective performance of the employee's official duties and responsibilities.

3. Participating in unauthorized political activities of any kind during working hours or while in uniform.

4. Favoring or discriminating against any employee or person seeking County employment because of political opinions or affiliations.

5. Participating in political activities in a manner so as to represent the County or any of its departments, officers, agencies, or officials, as endorsing a ballot measure, if such endorsement has not previously been given publicly.

6. Directly or indirectly using official authority or influence to interfere with any election.

7. Running for any political office, the campaign for which requires expenditures of such a substantial amount of the employee's time as to interfere with the effective performance of the employee's job, unless a leave of absence is secured by the employee upon declaration of intention to run.

8. Permitting any person to enter any facility under the employee's control for purpose of soliciting or receiving political funds or contributions.

9. Using a County office to confer benefits or detriments in return for political activity, votes or corrupt considerations.

10. Expending any public resources to promote any partisan position (this includes a prohibition of all signs and placards of a political nature on County property).

11. Using any County property, including computers and e-mail, for political activities.

In addition to the above, employees on "grant funded" items funded by the Federal government are restricted by the Hatch Act from running for partisan political office. Additionally, employees in services financed in whole or in part by loans or grants made by the Federal government may also be restricted from running for partisan political office.

Nothing in this policy shall be interpreted as denying any employee's right to vote, to express an opinion on any political matter, to participate in non-partisan political activities or engage in political activities during off-duty hours.

COUNTY OF LOS ANGELES
Public Health

SUBJECT: THREAT MANAGEMENT "ZERO TOLERANCE" POLICY	PAGE 1
	OF 4

POLICY No.: 746	EFFECTIVE DATE: 09/30/09
APPROVED BY: Jonathan Fielding MD	SUPERSEDES: DHS Policy No. 792

PURPOSE: To prevent threats/acts of violence by employees and clients at the workplace, and to ensure that all employees of the Department of Public Health (DPH) comply with the Department's Threat Management "Zero Tolerance" reporting requirements.

POLICY: All employees, including contract workers, students, agency personnel, volunteers, (whether they are permanent, temporary, part-time, or other), are entitled to a safe and healthy work environment. DPH prohibits any workplace threats, intimidation or harassment by any of its employees (as defined in this paragraph).

Threats, threatening behavior, acts of violence against employees, patients, visitors or other individuals by anyone on County property or anywhere an employee is engaged in County-related business, are prohibited. Examples of such behavior include but are not limited to:

- Verbal and/or written threats, including bomb threats, to a County facility or toward any employee and/or members of that person's family;
- Psychological violence such as bullying, verbal and/or written threats against any property of the persons listed above;
- Items left in an employee's work area or personal property that are meant to threaten or intimidate that person;
- Off-duty harassment of employees, such as phone calls, stalking, or any other behavior that could reasonably be construed as threatening or intimidating and that could affect workplace safety;
- Physical actions against another employee that could cause harm;
- Carrying a weapon on County property or while engaged in County business, as defined below.

Weapons

Employees shall not carry a prohibited weapon of any kind while in the course and scope of performing their job, whether or not they are personally licensed to carry a concealed weapon. Employees are prohibited from carrying a prohibited weapon anywhere on County property or at any County-sponsored function.

Prohibited weapons include any form of weapon or explosive restricted under local, state or federal regulation. This includes all firearms, illegal knives or other weapons prohibited by law.

Violations of this policy may result in any or all or the following:

- Arrest and prosecution for violations of pertinent laws
- Immediate removal of the threatening individual from the premises pending investigation
- Disciplinary action up to and including discharge from County employment.

Temporary Restraining Orders and Injunctions against Workplace Violence

Grounds for obtaining an injunction are based upon the definition of a credible threat of violence defined by the State of California as "a knowing and willful statement or course of conduct that would place a reasonable person in fear for his or her safety, or the safety of his or her immediate family, and that serves no legitimate purpose."

Requests for a court order to restrain actual or threatened workplace violence must first be reviewed and approved by the Department Head or designated representatives before referral to County Counsel.

Safety Concerns

Although only a minority of distressed or troubled employees pose a significant risk of becoming violent, workplace apprehension and concern about such employees is common. When no threat is expressed but a troubled employee arouses safety concerns, managers are encouraged to offer the confidential and free services of the Chief Executive Office, Employee Assistance Program (EAP) at (213) 738-4200. EAP referrals may be made to employees who show signs of disturbance or distress. Early identification and referral of such employees can avert the development of more serious problems.

Reporting Responsibilities

Any employee who witnesses any threatening or violent behavior, is a victim of, or has been told that another person has witnessed or was a victim or any threatening or violent behavior, is responsible for immediately reporting the incident to his/her supervisor or manager. Supervisors and managers shall document and maintain a log

of all incidents related to an expressed or implied threat involving an employee in the workplace, and will take appropriate action to ensure the safety of the threatened employee. Supervisors and managers shall ensure a Security Incident Report (SIR) (Attachment I) is completed by the person reporting or involved in the incident, Safety Police, facility security, or building manager and submitted to the Office of Security Management, Chief Executive Office by the end of the business day following the incident. A copy of the SIR should also be forwarded to the DPH Human Resources Employee Relations/Performance Management Unit.

In the case of home healthcare workers (such as Home Nursing Attendants or other in-home personal healthcare workers) any incident of violence must also be reported to the State of California Department of Industrial Relations, Division of Labor Statistics and Research – Illness and Injury Unit, at (415) 703-4780.

GUIDELINES:

The Director, DPH Human Resources shall establish procedures to ensure that employees are aware of this policy. Such procedures shall include, but are not limited to, the following:

1. Review of this policy with each incoming employee and documented in the personnel file.

2. Review of this policy by supervisor/manager and the employee at the time of the annual Performance Evaluation, in accordance with Performance Evaluation Policy.

3. Written notice provided to volunteers, contractors, and other non-compensated workers.

AUTHORITY: Department of Human Resources Policy No. 620
State of California Labor Code Section 6332
State of California Code of Civil Procedure Section 527.8

COUNTY OF LOS ANGELES * DEPARTMENT OF PUBLIC HEALTH
HUMAN RESOURCES

I acknowledge receipt of the Department of Public Health "Threat Management "Zero Tolerance" Policy regarding workplace violence.

My signature further acknowledges my understanding of my responsibilities under the Policy. I understand that my failure to adhere to this Policy may be grounds for disciplinary action up to and including discharge from County employment.

EMPLOYEE NAME: _____

EMPLOYEE NO: _____

EMPLOYEE'S SIGNATURE: _____

DATE: _____

COUNTY OF LOS ANGELES
Public Health

SUBJECT: DIVERSITY POLICY	PAGE 1
	OF 2

POLICY No.: 748	EFFECTIVE DATE: 3/31/10
APPROVED BY: Jonathan E. Fielding MD	SUPERSEDES: New

PURPOSE: To create a high performing, productive organization and an inclusive workplace environment in which each person is valued for his/her unique gifts and talents; to capitalize on the innovation inherent in diverse work groups; and to assure that each person is valued on individual characteristics rather than on stereotypes or assumptions.

POLICY: It is the policy of the Department of Public Health (DPH) to foster an environment in which:

1. Groups, as well as individuals, are appreciated for their differences and treat each other with respect;
2. Employees understand and appreciate the heritage and culture of many different groups and are responsive to the uniqueness of each individual;
3. Individuals reach beyond their own experience to appreciate and work effectively with people different from themselves; and
4. All employees reach their full potential in pursuit of departmental and organization objectives.

GOAL: A diverse work force provides advantages both internally, in terms of human resources potential offered by a variety of diverse perspectives, and externally, in increasing the Department's ability to serve an equally diverse community. In order to treat people fairly and provide equal opportunity, DPH seeks to accommodate and learn from the different perspectives and values that characterize diverse employees and clients. Therefore, it is the goal of DPH to:

1. Build on the foundation of equality of opportunity and diversity, and embrace these concepts as necessary to ensure fair representation and treatment of diverse employees and the multicultural community we serve;
2. Establish a strategic plan for managing diversity in every organization;
3. Ensure equal employment opportunity and upward mobility for all elements of our diverse work force;
4. Create an organization culture that fosters individual understanding and accountability for learning about and appreciating employee differences;
5. Make valuing diversity a core departmental and organizational value, one which is practiced and communicated at all levels of DPH;

6. Conduct employee training to instruct participants to respect the individuality of others by creating an openness to the experience of others, by generating awareness of personal perceptions, by imparting knowledge of cultural characteristics, and by teaching skills to apply cultural concepts in everyday working behaviors; and
7. Hold all managers accountable for demonstrating leadership in valuing diversity.

TRAINING:

1. All DPH employees must receive Diversity and Unlearning Prejudice training.
2. Each employee's attendance at this training must be documented.

RESPONSIBILITIES:

DPH Human Resources

1. DPH Human Resources will provide each newly appointed employee a copy of the DPH Diversity Policy, and obtain his/her signature acknowledging that he/she has received a copy of the policy, and will adhere to it.
2. DPH Human Resources will ensure the DPH Diversity Policy is reviewed annually, and acknowledged by the employee, as delineated in the "Agreement of Understanding" form which is to be attached to each employee's annual performance evaluation.
3. DPH Human Resources will be responsible for scheduling all of the required Diversity Policy training sessions.

AUTHORITY:

Los Angeles County Ordinances and Policies

- County of Los Angeles Ordinance 5.10 - Policy on Diversity

COUNTY OF LOS ANGELES
Public Health

SUBJECT:	**PUBLIC HEALTH INFORMATION TECHNOLOGY AND SECURITY POLICY**	**PAGE**	1
		OF	16

POLICY No.: 1000	**EFFECTIVE DATE:** 04/15/09
APPROVED BY:	**SUPERSEDES:** DHS Policy No. 935

PURPOSE: To provide direction for the development and implementation of data security policies and procedures and to identify the data security officials and their responsibilities.

POLICY: The Department of Public Health (Public Health) is responsible for securing all electronic data, including Protected Health Information and other confidential information, while complying with the security requirements of all applicable regulatory, compliance and accreditation sources, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated there under, including the Security Standards for Electronic Protected Health Information at 45 Code of Federal Regulations (CFR) Parts 160 and 164, Medicare, Medi-Cal and JCAHO.

The term Public Health, as used in the Information Technology (IT) security policies 1000 series, refers to electronic Protected Health Information (ePHI).

Public Health must develop data security policies and procedures to ensure the security of Protected Health Information and other confidential information, and the hardware and systems used to obtain, utilize, and maintain such information.

All Public Health workforce members must comply with provisions of the Public Health data security policies. Any workforce member who fails to comply will be subject to disciplinary action in accordance with Public Health Policy No. 1201, Disciplinary Action for Failure to Comply with Privacy Policies and Procedures, Public Health Policy No. 741, Disciplinary Action, Civil Service Rule 18.031 and the Public Health Employee Evaluation and Discipline Guidelines.

Non-DPH County workforce members, contractors and agencies that violate the security policies and procedures are subject to sanctions or penalties imposed pursuant to the applicable contract or memorandum of understanding (MOU) and/or federal, state, local law.

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

Departmental Information Security Officer (DISO)

A. Public Health must designate a DISO who is responsible for the development, implementation and maintenance of Public Health data security policies, procedures, and guidelines.

B. The DISO will assist Public Health managers and/or designated staff in the risk analysis and management process.

C. The duties of the DISO include, but are not limited to the following:

1. Chair the Departmental Information Security Steering Committee (DISSC).

2. Provide information security related technical, regulatory, and policy leadership.

3. Facilitate the development and implementation of the Public Health information security policies and procedures.

4. Coordinate information security efforts across the Facilities/Programs within Public Health in alignment with Countywide security policies.

5. Direct continuing information security training and education efforts.

6. Represent Public Health at the County Information Security Steering Committee (ISSC).

7. Report to the Public Health Chief Information Officer (CIO).

8. Ensure Public Health is in compliance with all laws, rules and regulations as it relates to the proper handling of data and electronic media.

9. Recommend new security standards as technology changes.

10. Coordinate Public Health-wide security software and hardware purchasing and licensing.

11. Review and approve data security implementation and risk management efforts.

D. The DISO or designee must review and approve the Risk Analysis Report.

E. The DISO or designee must review and approve the Public Health Facility/Program Master Security Management Report, Public Health Policy No.1001, Security Management Process: Risk Management.

F. The DISO must assist Public Health Facility/Program System Managers/Owners in implementing the access authorization procedures and determining the appropriate technical access controls.

G. The DISO or designee will coordinate the Departmental Computer Emergency Response Team (DCERT).

H. The DISO or designee and DCERT are responsible for determining the appropriate level of response to a security incident.

The DISO or designee must represent the department at the County Computer Emergency Response Team (CCERT) as the primary department CERT member (DCERT).

Facility/Program IT Director and/or Program Director

The duties of the Facility/Program IT Director, Program Director, and/or designee must include:

A. Management responsibility over all systems within their facility.

B. Ensure that Public Health Facility/Program System Managers/Owners conduct risk assessments for their data resources and information systems in accordance with Public Health procedures.

C. Create and periodically update the Facility/Program Master Security Management Report.

D. Ensure that Public Health Facility/Program System Managers/Owners develop plans to implement the Facility/Program Master Security Management Report's recommended safeguards and actions.

E. Ensure that Public Health Facility/Program System Managers/Owners establish, document, and implement procedures for reviewing information systems activity, including but not limited to audit logs, problem logs, system access reports, change control logs, and security incident reports.

F. Work with Public Health Facility/Program System Managers/Owners, Public Health managers and supervisors and Public Health Human Resources to develop workforce security procedures and to coordinate those activities necessary to implement the workforce security procedures.

G. Ensure that Public Health Facility/Program System Managers/Owners authorize access to information resources under their control on a "need to know basis" for carrying out the essential job functions of the workforce members.

H. Ensure that Public Health Facility/Program System Managers/Owners implement procedures for establishing Public Health workforce member access to electronic information, for example, through access to a workstation, transaction, program, process, or other mechanism, that is both necessary and appropriate for the job functions of the workforce member.

I. Ensure that Public Health Facility/Program System Managers/Owners implement procedures that modify a user's right of access to a workstation, transaction, program, process, or other mechanism, when such modification is necessary to align the workforce members' access with the workforce members' essential job functions.

J. Ensure that the Public Health Facility/Program System Managers/Owners respond to security incidents and emergency situations in a manner authorized and directed by the DISO or designee and DCERT

Facility/Program Information Security Coordinator (FPISC)

Each Public Health Facility/Program within Public Health must designate a FPISC responsible for working with the DISO in the implementation and maintenance of the data security policies, procedures and guidelines.

The duties of the FPISC include, but are not limited to the following:

A. Manage information security within the facility

B. Coordinate the development, implementation, and update of facility specific information security policies

C. Represent the Facility/Program at the DISSC

D. Assist the Facility DCERT member in responding to and documenting security incidents

E. Coordinate the implementation of the Public Health information security policies

F. Monitor Risk Management effectiveness

G. Report to the Facility/Program IT Director and/or Program Director

Departmental Information Security Steering Committee (DISSC)

The DISO and the FPISC will designate the members of the DISSC that must develop the appropriate security strategies for Public Health, taking into consideration the balance between heightened security and the Department's need to carry out its mission.

The DISSC's responsibilities are as follows:

A. Along with the DISO develop, review, recommend and update information security policies and procedures.

B. Develop, review, and recommend best practices, standards, and guidelines.

C. Develop, review, and recommend security awareness and training program.

D. Coordinate Inter-Facility communication and collaboration.

E. Recommend compliance self-evaluation.

F. Review compliance and audit documentation and ensure recommendations are implemented in a timely manner.

Public Health Facility/Program System Managers/Owners

Public Health Facility/Program System Managers/Owners security responsibilities include, but are not limited to, the following:

A. Establish rules for system use and protection of the Public Health and other confidential information as required in Public Health Policy No. 1201 Public Health Privacy and Security Compliance Program.

B. Work with Public Health Facility/Program IT Director and/or Program Director to develop and implement the Public Health Policy No. 1001, Security Management Process: Risk Management.

C. Establish, document, and implement procedures for reviewing information systems activity, including but not limited to audit logs, problem logs, system access reports, change control logs, and security incident reports.

D. Work with Public Health Facility/Program IT Director, Program Manager or designee, Public Health managers and supervisors and Public Health Human Resources to develop workforce security procedures and to coordinate those activities necessary to implement the workforce security procedures.

E. Implement procedures for establishing Public Health workforce member access to electronic information, for example, through access to a workstation, transaction, program, process, or other mechanism, that is both necessary and appropriate for the job functions of the workforce member.

F. Ensure that each workforce member with access has signed an acknowledgment of Public Health Policy No. 1016, Acceptable Use Policy for County Information

Technology Resources that defines their responsibility for protecting the confidentiality, integrity and availability of all Public Health information resources and identifying restrictions for utilizing those resources.

G. Determine the sensitivity and criticality of the resources for which they are responsible and develop, implement and maintain the Contingency Plan (CP) that commensurate with the criticality.

H. Ensure that appropriate physical safeguards and technical security policies are implemented.

J. Define the system's security requirements in a System Security Documentation.

K. Train and communicate to the workforce member the proper procedures for protecting the Public Health and other confidential information.

Public Health Human Resources (HR)

The security responsibilities of the Public Health Human Resources must include:

A. Work with Public Health Facility/Program System Managers/Owners to ensure proper workforce clearance procedures are implemented. Refer to Public Health Policy No. 723, Criminal Records Background Check/ Fingerprinting Policy.

B. Ensure that each new workforce member receives and signs acknowledgment of Public Health Policy No. 1016, Public Health Acceptable Use Policy for County Information Technology Resources during the new-hire orientation and that each workforce member completes the acknowledgment during the annual Performance Evaluation process. Signed acknowledgments will be filed in the workforce member's official personnel folder.

Workforce Managers and Supervisors

The security responsibilities of workforce managers and supervisors must include:

A. Determine workforce members' access rights and levels based on the workforce members' job responsibilities and authorize workforce members' access to electronic data systems, the Internet and Intranet systems.

B. Supervise the activities of Public Health workforce members in relation to the use and disclosure of electronic data.

C. Provide authorization and supervision to workforce members and others who need to be in areas where confidential and sensitive information may be accessed and take appropriate safeguards to ensure those who may be exposed

to confidential or sensitive information are made aware of the policies protecting that information.

D. Identify and supervise workforce members who work with confidential and/or sensitive information or who work in locations where confidential and/or sensitive information might be accessed.

Workforce Member

The security responsibilities of all Public Health workforce members must include:

A. Complying with the provisions of all relevant data security policies and procedures. Including but not limited to Public Health Policy No. 1201, Privacy and Security Compliance Program, Public Health Policy No. 1016, Acceptable Use Policy for County Information Technology Resources, and Public Health Policy No. 1008, Workstation Use and Security.

B. Reporting any and all suspected and actual breaches of information security to the Public Health DCERT.

DEFINITIONS:

Terms used in this policy and subsequent Public Health data security policies and procedures are included in the Public Health Information Security Glossary (Attachment I).

AUTHORITY: 45 code of Federal Regulations (CFR) Parts 160 and 164
Health Insurance Portability and Accountability Act of 1996 (HIPAA) Public Law 104-91
Board of Supervisor's Policies:
6.100 Information Technology and Security Policy

REFERENCE: Board of Supervisors Policies:
6.101 Use of County Information Technology Resources
6.102 Countywide Antivirus Security Policy
6.103 Countywide Computer Security Threat Response
6.104 Use of Electronic Mail (e-mail) by County Employees
6.105 Internet Usage Policy
6.106 Physical Security
6.107 Information Technology Risk Assessment
6.108 Auditing and Compliance
6.109 Security Incident Reporting
6.110 Protection of Information on Portable Computing Devices
6.111 Information Security Awareness Training
6.112 Secure Disposition of Computing Devices

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

ACCESS TO INFORMATION	The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.
ACCESS LEVELS	1) In security, the level of authority required from an entity to access a protected resource. Note: An example of access level is the authority to access information at a particular security level. 2) The hierarchical portion of the security level used to identify sensitivity of information-system (IS) data and the clearance or authorization of users. Access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. (INFOSEC) -Telecom Glossary 2K
ACCESS RIGHTS	The privilege to use computer information in some manner. For example, a user might be granted read access to a file, meaning that the user can read the file but cannot modify or delete it. Most operating systems have several different types of access privileges that can be granted or denied to specific users or groups of users. (Webopedia)
ADMINISTRATIVE SAFEGUARDS	Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect Protected Health Information and confidential and/or sensitive information and to manage the conduct of Public Health's workforce in relation to the protection of that information.
APPLICATION	Any program designed to perform a specific function directly for the user or, in some cases, for another application program. Examples of application programs include word processors; database programs; Web browsers; development tools; drawing, paint, and image editing programs; and communication programs.
AUDIT TRAILS	A data security system should maintain detailed logs of who did what and when and also if there are any attempted security violations. Logs provide information that allows the system auditor to determine who initiated the transaction, the time of the day and date of entry, the type of entry, what fields were affected, and the terminal used.
AUTHENTICATION	The validation of the identify of the user.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

AVAILABILITY	Assurance that there exists timely, reliable access to data by authorized entities, commensurate with mission requirements.
CCERT	Los Angeles County's Computer Emergency Response Team that has responsibility for response and reporting of Information Technology (IT) security incidents.
CERT	Computer Emergency Response Team that has responsibility for response and reporting of IT security incidents within an organization.
COMPUTER SYSTEM	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.
CONFIDENTIALITY	Assurance that data is protected against unauthorized disclosure to individuals, entities, or processes.
CONTINGENCY PLAN	A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan.
CONTINGENCY PLANNING	A planned response to high impact events to maintain a minimum acceptable level of operation.
DATA	A collection of observations of fact.
DATABASE	A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; data is stored so that it can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data.
DCERT	Departmental Computer Emergency Response Team. The Department's CERT that has responsibility for response and reporting of IT security incidents.
DEVICE	Any equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
PUBLIC HEALTH INFORMATION RESOURCES	Los Angeles County Department of Public Health's computer systems. See definition of *computer systems* above.
DISASTER RECOVERY	A plan for the restoration of lost data, or the reconciliation of conflicting or erroneous data, after a system failure due to natural or manmade disaster.
DISO	Los Angeles Department of Public Health's Information Security Officer
ELECTRONIC INFORMATION SYSTEMS	An automated set of methods, software, and hardware that operates as a whole to accomplish a prescribed task with regard to data.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)	1) Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; (2) Protected health information excludes individually identifiable health information in: (i) Education records (ii) Employment records held by a covered entity in its role as employer. 2) Protected Health Information that is transmitted by electronic media or is maintained in electronic media. This does not include health information contained in employment records held by Public Health in its role as employer.
ENCRYPTION	The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission, or when it is stored on a transportable magnetic medium. (Microsoft Press Computer Dictionary)
EPHI	See, Electronic Protected Health Information
FACILITY	Facility encompasses all locations where there are Public Health Programs, Offices, Clinics, or administrative offices.
FACILITY CHIEF INFORMATION OFFICER (Facility CIO)	A Chief Information Officer in a Public Health Facility.
FACILITY INFORMATION SECURITY COORDINATOR (FISC)	A person with the responsibility for information security in a Public Health Facility.
FACILITY PRIVACY COORDINATOR/OFFICER	A person with the responsibility for privacy in a Public Health Facility.
GUIDELINES	General statements that are designed to achieve the policy's objectives by providing a framework within which to implement procedures.
HYBRID ENTITY	A single legal entity that acts as provider and health care plan.
ILLEGAL ACCESS AND DISCLOSURE	Activities of employees that involve improper systems access and sometimes disclosure of information found thereon, but not serious enough to warrant criminal prosecution.
INCIDENT	An occurrence or event that interrupts normal procedure or precipitates a crisis.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

INFORMATION	Any communication or reception of knowledge, such as facts, data, or opinions; including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape.
INFORMATION TECHNOLOGY (IT)	A term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, personal health information, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).
INFORMATION TECHNOLOGY ASSETS/RESOURCES	See definition of computer system above.
INTEGRITY	Assurance that data is protected against unauthorized, unanticipated, or unintentional modification and/or destruction.
INTEGRITY CONTROL	The mechanism or procedure that assures data or information is protected against unauthorized, unanticipated, or unintentional modification and/or destruction.
INTERNET	A worldwide electronic system of computer networks which provides communications and resource sharing services to government employees, businesses, researchers, scholars, librarians and students as well as the general public.
LOCAL AREA NETWORK (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network (Microsoft Press Computer Dictionary) Local Area Networks commonly include microcomputers and shared resources such as laser printers and large hard disks. Most modem LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks.
MALICIOUS SOFTWARE	The collective name for a class of programs intended to disrupt of harm systems and networks. The most widely know example of malicious software is the computer virus; other examples are Trojan horses and worms.
MEDIA	Hard copy (including paper), PC/workstation diskettes, and other electronic forms by which data is stored, transported, and exchanged. The need to protect information confidentiality, integrity, and availability applies regardless of the medium used to store the information. However, the risk exposure is considerably greater when the data is in an electronically readable or transmittable form compared to when the same data is in paper or other hard copy form.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

MODEM	Modem is short for modulator/demodulator, a communications device that enables a computer to transmit information over a standard telephone line. Modems convert digital computer signals into analog telephone signals (modulate) and the reverse (demodulate). (Microsoft Press Computer Dictionary)
NETWORK	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables or temporary connections made through telephone or other communications links. A network can be as small as a LAN consisting of a few computers, printers and other devices, or it can consist of many small and large computers distributed over a vast geographic area. Small or large, a computer network exists to provide computer users with a means of communicating and transferring information electronically. (Microsoft Press Computer Dictionary)
PASSWORDS	A confidential character string used to authenticate an identity or prevent unauthorized access. (FISCAM) Passwords are most often associated with user authentication. However, they are also used to protect data and applications on many systems, including PCs. Password-based access controls for PC applications are often easy to circumvent if the user has access to the operating system (and knowledge of what to do).
PERIODIC	Recurring from time to time; intermittent.
PERSONNEL SECURITY	Personnel security refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of resources which the individual will be able to access.
PHI	See Protected Health Information
PHYSICAL SECURITY	The application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information.
POLICY	A high-level statement of departmental beliefs, goals, and objectives and the general means for their attainment for a specified subject area.
PROCEDURES	Define the specifics of how the policy and the supporting standards and guidelines will actually be implemented in an operating environment.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

PROTECTED HEALTH INFORMATION (PHI)	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. Protected health information excludes individually identifiable health information in education records and employment. The term PHI, as used in the IT security policies 1000 series, refers to electronic Protected Health Information.
RISK	The potential for harm or loss. Risk is best expressed as the answers to these four questions: (1) What could happen? (What is the threat?) (2) How bad could it be? (What is the impact or consequence?) (3) How often might it happen? (What is the frequency?) (4) How certain are the answers to the first three questions? (What is the degree of confidence?) The key element among these is the issue of uncertainty captured in the fourth questions. If there is no uncertainty, there is no "risk" per se.
RISK ASSESSMENT	The identification and study of the vulnerability of a system and the possible threats to its security.
RISK MANAGEMENT	The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.
SAFEGUARDS	Administrative, physical and technical actions or measures, and policies and procedures to protect Protected Health Information (PHI) and other confidential information.
SECURITY	All of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from outside and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data. (HIPAA Security Standard)

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

SECURITY LEVEL DESIGNATION	A rating based on the sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse), and the operational criticality of data processing capabilities (i.e., the consequences where data processing capabilities to be interrupted for some period of time or subjected to fraud or abuse). There are four security level designations for data sensitivity and four security level designations for operational criticality. The highest security level designation for any data or process within an information system is assigned for the overall security level designation.
SECURITY VIOLATION	An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources. This includes, but is not limited to, unusual or apparently malicious break-in attempts (either local or over a network), virus or network worm attacks, or file or data tampering, or any incident in which a user, either directly or by using a program, performs unauthorized functions.
SENSITIVE DATA	Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission (e.g., proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.).
SENSITIVE INFORMATION	Any information that, if lost, misused, accessed or modified in an improper manner, could adversely affect the county interest, the conduct of county programs, or the privacy to which individuals are entitled.
SEPARATION OF DUTIES	Separation of duties refers to the policies, procedures, and organizational structure that help ensure one individual cannot independently control all key aspects of a process or computer-related operation. Independent control would enable the individual to conduct unauthorized actions or gain unauthorized access to assets or records without detection. Strict controls involving the maintenance or use of IT assets would ensure that no individual has the ability to both perpetrate and conceal an accidental or intentional breach of IT security.
SIGNIFICANT CHANGE	A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a LAN, changing from batch to online processing, adding dial-up capability, and increasing the equipment capacity of the installation. (DHHS Definition)
STANDARDS	Mandatory activities, actions, rules, or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

SYSTEM	A set of integrated entities that operate as a whole to accomplish a prescribed task.
SYSTEM LIFE CYCLE	The period of time beginning when the software product is conceived and ending when the resultant software products are no longer available for use. The system lifecycle is typically broken into phases, such as requirements, design, programming and testing, installation, and operations and maintenance. Each phase consists of a well-defined set of activities whose products lead to the evolution of the activities and products of each successive phase.
SYSTEM MANAGER/OWNER	The person who is responsible for the operation and use of a system.
SYSTEM SECURITY PLAN	A basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements.
TECHNICAL SAFEGUARDS	The technology and the policy and procedures for its use that protect confidential and/or sensitive information and control access to it.
TELECOMMUNICATIONS	A general term for the electronic transmission of information of any type, including data, television pictures, sound, and facsimiles, over any medium such a telephone lines, microwave delay, satellite link, or physical cable.
THREAT	An entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses.
THREAT IDENTIFICATION	The analysis of recognized threats to determine the likelihood of their occurrence and their potential to harm assets.
USER	The person who uses a computer system and its application programs to perform tasks and produce results. (FISCAM) Any organizational or programmatic entity that utilizes or receives services from a facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or supervisor or director of the facility or to the same immediate supervisor.
VIRUS	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executable when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating competent.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

VULNERABILITY	A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.
WIDE AREA NETWORK (WAN)	1) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. (FISCAM) 2) A WAN is a communications network that connects geographically separated areas (Microsoft Press Computer Dictionary.
WORKFORCE MEMBER	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 department.
WORKSTATION	A workstation is a computer built around a single-chip microprocessor. Less powerful than minicomputers and mainframe computers, workstations have nevertheless evolved into very powerful machines capable of complex tasks. Technology is progressing so quickly that state-of-the-art workstations are as powerful as mainframes of only a few years ago, at a fraction of the cost. (Microsoft Press Computer Dictionary)
WORM	A worm is a program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system either for fun or with intent to damage or destroy information.

RESOURCE ACRONYMS

CMS (Centers for Medicare & Medicaid Services)
DHHS (U.S. Department of Health and Human Services)
FISCAM (Federal Information Security Controls Audit Manual)
HIPAA (Health Insurance Portability and Accountability Act of 1996)
INFOSEC (National Information Systems Security Glossary)

COUNTY OF LOS ANGELES
Public Health

SUBJECT:	ACCEPTABLE USE POLICY FOR COUNTY INFORMATION TECHNOLOGY RESOURCES	PAGE 1 OF 7

POLICY No.: 1016	EFFECTIVE DATE: 04/15/09
APPROVED BY: J E Fielding	SUPERSEDES: DHS Policy No. 935.20

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

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

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

Public Health System Managers/Owners will ensure that all Users with access to County information technology resources have signed the agreement and acknowledgment prior to providing access.

I. RESPONSIBILITY

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

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

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

II. WORKFORCE MEMBER PRIVACY

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

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

III. PROHIBITED ACTIVITIES

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

1. Engaging in unlawful or malicious activities;

2. Sending, receiving or accessing pornographic materials;

3. Engaging in abusive, threatening, profane, racist, sexist or otherwise objectionable language;

4. Misrepresenting oneself or the County;

5. Misrepresenting a personal opinion as an official County position;

6. Defeating or attempting to defeat security restrictions on County systems or applications;

7. Engaging in personal or commercial activities for profit;

8. Sending any non-work related messages;

9. Broadcasting unsolicited, non-work related messages (spamming);

10. Intentionally disseminating any destructive program (e.g., viruses);

11. Playing games or accessing non-business related applications;

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

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

14. Using County information technology resources to gain unauthorized access to Public Health's or other systems;

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

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

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

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

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

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

B. Misuse of software: At no time must Users be engaged in software copyright infringements. Users are prohibited from conducting the following activities without proper licensing and prior written authorization by the Facility CIO/designee:

1. Copying County-owned software onto their home computers;

2. Providing copies of County-owned software to independent contractors, clients or any other third-party person;

3. Installing software on any Public Health workstation (e.g., desktops, personal computers, mobile devices, laptops) or server;

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

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

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

IV. PASSWORDS

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

V. SECURITY

A. County information technology resources

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

B. Malicious software

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

Any User who telecommutes or is granted remote access must utilize equipment that contains current County-approved anti-virus software and must adhere to County hardware/software protection standards and procedures that are defined by the County and the authorizing Department.

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

Each User is responsible for notifying the Department's Help Desk or the Department Security contact as soon as a device is suspected of being compromised by a virus.

VI. E-MAIL

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

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

Protected Health Information (PHI) and other confidential and/or sensitive information can only be sent or received if it is encrypted or safeguarded in accordance with Public Health Policy No. 1223, Safeguards for Protected Health information (PHI), G. Use of Electronic Systems, 2) E-mail and Attachment 1, Public Health Guidelines Governing the Use of E-Mail Involving Protected Health Information (PHI).

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

VII. USE OF THE INTERNET

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

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

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

VIII. RECORDABLE MOBILE DEVICES AND REMOVABLE MEDIA

Users must manage and control and ensure encryption, as per County standard, of all recordable mobile devices and removable media that contain PHI or other confidential information. These devices include PDA's, USB flash drives, cellular phones, cameras and camera phones, removable hard-disks, CD-R, CD-RW, DVD-R, DVD-RW and floppy disks.

The use of recordable mobile devices and removable media must be pre-approved and registered for use by the Facility CIO/designee in accordance with Public Health Policy No. 1008, Workstation Use and Security: Access and Use of Mobile Devices.

DEFINITIONS:

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

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

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

AUTHORITY: Board of Supervisors Policies:
6.101, Use of County Information Technology Resources
6.102, Countywide Antivirus Security Policy
6.104, Use of Electronic Mail (e-mail) by County Employees
6.105, Internet Usage Policy
6.110, Protection of Information on Portable Computing Devices

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

COUNTY OF LOS ANGELES
Public Health

SUBJECT:	**EXCLUSION OF INDIVIDUALS/ENTITIES FROM FEDERAL HEALTH CARE PROGRAMS**	**PAGE** 1 **OF** 3
POLICY No.: 1103		**EFFECTIVE DATE:** 10/15/10
APPROVED BY:		**SUPERSEDES:** DHS Policy No. 1001

PURPOSE: To prevent the employment of, or contracting with, an individual or entity that is excluded from participation in Federal health care programs by the Office of Inspector General (OIG) of the Department of Health and Human Services or excluded from Federal procurement and non-procurement programs as reported by the United States General Services Administration (GSA). The GSA maintains a list of parties debarred, suspended, proposed for debarment, or declared ineligible by Federal Agencies or by the Government Accounting Office.

POLICY: The Department will not knowingly employ, contract with, or purchase from individuals or entities that are excluded by the OIG or appear on the GSA's exclusion list. Prior to entering into employment or contractual relationships, and periodically thereafter, the Department will check the exclusion status of individuals and contracting entities.

All DPH employees and contractors are required to report to their supervisor or Program Liaison, respectively, if, subsequent to their employment or engagement through contract, they become subject to exclusion. Employees and contractors must also report to their supervisor or Program Liaison if they become aware that another employee or contractor has become subject to exclusion.

DPH will terminate any employment or contract agreement with any individuals or entities that are found to be excluded by the OIG or that appear on the GSA's exclusion list.

The Director of Public Health or his designee's written approval is required to waive the requirements of this policy in appropriate circumstances.

GUIDE: Non-compliance with the policy could subject the Department to civil monetary penalties under the Federal Social Security Act and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Additionally, the Department cannot receive reimbursement from a Federal health care program (e.g., Medi-Cal, Medicare, etc.) for services provided by or ordered by an individual who the Department knows, or should have known, is excluded from program participation.

PROCEDURES:

The following procedures must be implemented to prevent the employment of, or contracting with, excluded individuals or entities.

DPH Human Resources

- Check the OIG's List of Excluded Individuals/Entities on the OIG web site (www.hhs.gov/oig) and the GSA's List of Parties Excluded from Federal Procurement and Nonprocurement Programs (http://epls.arnet.gov/) prior to hiring employees or utilizing contract staff that provide services on-site at DPH facilities.

- Annually check the OIG's List of Excluded Individuals/Entities and the GSA's List of Parties Excluded from Federal Procurement and Nonprocurement Programs to determine the exclusion status of current employees and on-site contract staff. Immediately report any excluded individuals/entities to the Department's Audit and Investigation Division for necessary action.

- Prior to employment, require potential employees to certify that they are not presently excluded or at risk of exclusion as a result of an existing or recently completed investigation by the State or Federal Governments.

- At the start of service, notify employees of their ongoing obligation to report to their supervisors if they, or another employee that they are aware of, becomes subject to an exclusion. Employees who do not comply with this obligation may be subject to disciplinary action, in accordance with the Department's "Employee Evaluation and Discipline Guidelines".

Contracts and Grants

- Ensure that Department contracts include language requiring contractors to certify that neither they nor any of their staff members performing services for the Department are excluded from providing services to beneficiaries of a Federal health care program or suspended, debarred, ineligible, or excluded from securing federally funded contracts to notify the County immediately of any exclusionary action taken or any event that would require contractor or a staff member's exclusion.

- Check the OIG's List of Excluded Individuals/Entities and the GSA's List of Parties Excluded from Federal Procurement and Nonprocurement Programs prior to entering into any contracts to determine the exclusion status of the contractor.

Materials Management

- Check the OIG's List of Excluded Individuals/Entities and the GSA's List of Parties Excluded from Federal Procurement and Nonprocurement Programs prior to issuing purchase orders with any new vendor to determine the vendor's exclusion status.

- Require all vendors to certify that they are not presently excluded or presently at risk of exclusion as a result of an existing or recently completed investigation by the State or Federal governments. This certification is not required of vendors with a contractual relationship with Novation.

- Require vendors to notify the County immediately of any exclusionary action taken or any event that would require the vendor's exclusion. This notification is not required of vendors with a contractual relationship with Novation.

Corporate Office of Purchasing and Standardization

Ensure that an annual check of the OIG's List of Excluded Individuals/Entities and the GSA's List of Parties Excluded from Federal Procurement and Nonprocurement Programs is conducted to determine the exclusion status of current vendors and contractors. Immediately report any excluded individuals/entities to the Department's Audit and Investigation Division for necessary action.

Audit and Investigation Division

- If it is determined that an employee, contractor/vendor or contractor's staff is excluded, Audit and Investigation will work with Human Resources, Contracts and Grants, Materials Management and/or County Counsel (as applicable) to coordinate the individual's/entity's termination of service and ensure any other corrective actions are taken (e.g., correction of any improper claims).

- If the Department becomes aware that an employee, contractor or contract staff is being investigated for actions that could lead to their exclusion, Audit and Investigation will work with the impacted area's management to determine the need to suspend or change the individual's/contractor's responsibilities pending the conclusion of the investigation to ensure that patient care is not adversely affected and that improper claims are not submitted.

Non-compliance with this policy should be reported to:

Audit and Investigation Division
5555 Ferguson Drive
Suite 320-24C, Room 3033
Commerce, CA 90022
(323) 869-8920 telephone or (323) 869-8919 via facsimile

AUTHORITY: Civil Monetary Penalties Law, 42 USC Section 1320a-7a(a)(5), 42 USC 1395y(e); 1396a(a)(39), 42 CFR Section 1001.1901, 45 C.F.R. Part 76

CROSS REFERENCES: Employee Evaluation and Discipline Guidelines

COUNTY OF LOS ANGELES
LOBBYINST ORDINANCE
(ORDINANCE NUMBER 93-0031)

NOTICE TO EMPLOYEES
ACCEPTANCE OF GIFTS PROHIBITIONS

All County employees whose duties involve responsibilities other than clerical or manual functions must be aware of the following gift prohibition statement.

Section 2.160.120 GIFT PROHIBITION. No county lobbyist or county lobbying firm shall make to a county official and no county official shall knowingly receive from a registered county lobbying firm a gift or gifts aggregating more than fifty dollars ($50) in any calendar month. No county lobbyist or lobbying firm shall act as an agent or intermediary in the making of any such gift or arrange for the making only such gift by any other person.

CHILD ABUSE REPORTING
ELDER/DEPENDENT ADULT ABUSE REPORTING
DOMESTIC/INTIMATE PARTNER VIOLENCE REPORTING
SEXUAL ABUSE/SEXUAL COERCION/SEXUAL MISCONDUCT
REPORTING SUSPICIOUS INJURIES

The following policy statements apply to all Los Angeles County Workforce Members. "Workforce Members" includes employees, volunteers, trainees, and any other persons who perform work under the control of Department of Public Health (DPH), whether or not they are paid by the County. "Employ/employment" as referenced in the statements below includes non-County workforce members assignments to a DPH Program.

CHILD ABUSE REPORTING

California Penal Code Section 11166.5 requires Los Angeles County DPH to provide all mandated reporters who commence employment or are assigned to a Los Angeles County DPH facility on and after January 1, 1985, with the following statement. California law requires this statement to be signed by the workforce member as a prerequisite to employment or assignment and be retained by Los Angeles County DPH.

> Section 11166 of the Penal Code requires a mandated reporter who, in his/her professional capacity or within the scope of his/her employment or assignment, has knowledge of or observes a child whom the mandated reporter knows or reasonably suspects has been the victim of child abuse or neglect to report the known or suspected abuse immediately or as soon as practicably possible by telephone and to prepare and send, fax or electronically submit a written follow-up report thereof within 36 hours of receiving the information concerning the incident. The report shall be prepared on the Department of Justice (DOJ) Form SS8572 may include any non-privileged documentary evidence the mandated reporter possesses related to the incident.

If after reasonable efforts, a mandated reporter is unable to submit an initial report by telephone, he or she shall immediately or as soon as practicably possible, by fax or electronic submission, make a one-time automated written report on the DOJ Form SS8572 and shall also be available to respond to a telephone follow-up call by the agency in which he or she filed the report. The report must also indicate the reason why the mandated reporter was not able to make an initial report by telephone.

Reports of suspected child abuse or neglect pursuant to Section 11166 or Section 11166.05 shall include the name, business address, and telephone number of the mandated reporter; the capacity that makes the person a mandated reporter; and the information that gave rise to the reasonable suspicion of child abuse or neglect and the source or sources of that information. If a report is made, the following information, if known, shall also be included in the report: the child's name, the child's address, present location, and, if applicable school, grade, and class; the names, addresses, and telephone numbers of the child's parents or guardians; and the name, address, telephone number, and other relevant personal information about the person or persons who might have abused or neglected the child. The mandated reporter shall make a report even if some of this information is not known or is uncertain to him or her.

This reporting requirement exists even if the child has expired, regardless of whether or not the possible abuse was a factor contributing to the death, and even if the suspected abuse was discovered during an autopsy.

The identity of all persons who report under these provisions shall be confidential and disclosed only among agencies receiving or investigating mandated reports, to the prosecutor in a criminal prosecution or in an action initiated under Section 602 of the Welfare and Institutions Code arising from alleged child abuse, or to counsel appointed pursuant to subdivision (c) of Section 317 of the Welfare and Institutions Code, or to the county counsel or prosecutor in a proceeding under Part 4 (commencing with Section 7800) of Division 12 of the Family Code or Section 300 of the Welfare and Institutions Code; or to a licensing agency when abuse or neglect in out-of-home care is reasonably suspected, or when those persons waive confidentiality, or by court order.

Reports of suspected child abuse or neglect shall be made by mandated reporters to the local law enforcement agency, county probation or county welfare departments. Child abuse reports may be made directly to the Los Angeles County Department of Children and Family Services (DCFS) through their website at http://dcfs.co.la.ca.us or their 24-hour hotline at (800) 540-4000. Written reports may also be faxed to DCFS at (213) 639-1321.

DEFINITIONS

Mandated Reporter – A teacher, An instructional aide, A teacher's aide or teacher's assistant employed by any public or private school, A classified employee of any public school, An administrative officer or supervisor of child welfare and attendance, or a certificated pupil personnel employee of any public or private school, An administrator of a public or private day camp, An administrator or employee of a public or private youth center, youth recreation program, or youth organization, An administrator or employee of a public or private organization whose duties require direct contact and supervision of children, An employee of a county office of education or the California Department of Education, whose duties bring the employee into contact with children on a regular basis, A licensee, an administrator, or an employee or a licensed community care or child day care facility, A Head Start program teacher, A licensing worker or licensing evaluator employed by a licensing agency as defined in Section 11165.11,

A public assistance worker, An employee of a child care institution, including, but not limited to, foster parents, group home personnel, and personnel of residential care facilities, A social worker, probation officer, or parole officer, An employee of a school district police or security department, Any person who is an administrator or presenter of, or a counselor in, a child abuse prevention program in any public or private school, A district attorney investigator, inspector, or local child support agency caseworker unless the investigator, inspector, or caseworker is working with an attorney appointed pursuant to Section 317 of the Welfare and Institutions Code to represent a minor, A peace officer, as defined in Chapter 4.5 (commencing with Section 830) of Title 3 of Part 2, who is not otherwise described in this section,

A firefighter, except for volunteer firefighters,

A physician, surgeon, psychiatrist, psychologist, dentist, resident, intern, podiatrist, chiropractor, licensed nurse, dental hygienist, optometrist, marriage, family, and child counselor, clinical social worker or any other person who is currently licensed under Division 2 (commencing with Section 500) of the Business and Professions Code, Any emergency medical technician I or II, paramedic, or other person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code, A psychological assistant registered pursuant to Section 2913 of the Business and Professions Code, A marriage, family, and child therapist trainee, as defined in subdivision (c) of Section 4980.03 of the Business and Professions Code, An unlicensed marriage, family and child therapist intern registered under Section 4980.44 of the Business and Professions Code, A state or county public health employee who treats a minor for venereal disease or any other condition,

A coroner, A medical examiner, or any other person who performs autopsies, A commercial film and photographic print processor, as specified in subdivision (e) of Section 11166. As used in this article, "commercial film and photographic print processor" means any person who develops exposed photographic film into negatives, slides, prints, or who makes prints from negatives or slides, for compensation. The term includes any employee of such a person; it does not include a person who develops film or makes prints for a public agency, a child visitation monitor. As used in this article, "child visitation monitor" means any person who, for financial compensation, acts as monitor of a visit between a child and any other person when the monitoring of that visit has been ordered by a court of law.

Animal control officer or humane society officer. For the purposes of this article, the following items have the following meanings:

(A) "Animal control officer" means any person employed by a city, county, or city and county for the purpose of enforcing animal control laws or regulations.
(B) "Humane society officer" means any person appointed or employed by a public or private entity as a humane officer who is qualified pursuant to Section 14502 or 14503 of the Corporations Code.

A clergy member, specified in subdivision (d) of Section 11166. As used in this article, "clergy member" means a priest, minister, rabbi, religious practitioner, or similar functionary of a church, temple, or recognized denomination or organization, Any custodian of records of a clergy member, as specified in this section and subdivision (d) of Section 11166,

Any employee of any police department, county sheriff's department, county probation department, or county welfare department, An employee or volunteer of a Court Appointed Special Advocate program, as defined in Rule 1424 of the California Rules of Court, A custodial officer as defined in Section 831.5,

Any person providing services to a minor child under Section 12300 or 12300.1 of the Welfare and Institutions Code.

Except as provided in paragraph (35) of subdivision (a), volunteers of public or private organizations whose duties require direct contact with and supervision of children are not mandated reporters but are encouraged to obtain training in the identification and reporting of child abuse and neglect and are further encouraged to report known or suspected instances of child abuse or neglect to any agency specified in Section 11165.9. Child abuse reports may be made directly to the DCFS through their website at http://dcfs.co.la.ca.us or their 24-hour hotline at (800) 540-4000.

Employers are strongly encouraged to provide their mandated reporters with training in the duties of a mandated reporter: identification and reporting of child abuse and neglect. School districts that do not train their mandated reporters must report the reasons why it was not done to the State Department of Education. Public and private organizations are encouraged to provide their volunteers whose duties involve direct contact with and supervision of children with training on identification and reporting of child abuse and neglect. Absence of the training does not excuse a mandated reporter from fulfilling their duties under these provisions.

Child – A "child" is defined as a person under the age of 18 years of age (Section 11165).

Child abuse or Neglect – includes physical injury inflicted by other than accidental means upon a child by another person, sexual abuse, neglect, the willful harming or injuring of a child or the endangering of the person or health of a child (child endangerment), and unlawful corporal punishment or injury. Child abuse or neglect does not include a mutual physical altercation between minors or injury caused by reasonable and necessary force used by a police officer acting in the scope of his or her employment as a police officer.

- Sexual Abuse – includes sexual assault or physical exploitation as defined in Section 11165.1 Neglect – the negligent treatment or the maltreatment of a child by a person responsible for the child's welfare under circumstances indicating harm or threatened harm to the child's health or welfare. The term includes both acts and omissions on the part of the responsible person. General neglect includes the failure of a responsible person to provide adequate food, clothing, shelter, medical care, or appropriate supervision. A child receiving medical treatment through spiritual means cannot be automatically determined to be neglected on that basis.
- Willful Harming or Injuring/Endangering – the responsible person causes or permits any child to suffer, inflicts unjustifiable physical pain or mental suffering, or in having the care and custody of any child, willfully causes or permits the person or health of the child to be placed in a situation in which his or her person or health is endangered.
- Unlawful Corporal Punishment or injury – willfully inflicting upon any child by cruel or inhumane corporal punishment or injury resulting in a traumatic condition. Does not include reasonable force needed by a person employed by or engaged in public school to quell a disturbance, self defense, to take control of a weapon or other dangerous object or device.

Reasonable Suspicion – it is objectively reasonable for a person to entertain a suspicion, based upon facts that could cause a reasonable person in a like position, drawing, when appropriate, on his or her training and experience, to suspect child abuse or neglect. For the purpose of this article, the pregnancy of a minor does not in, and of itself, constitute a basis for reasonable suspicion of sexual abuse.

ELDER/DEPENDENT ADULT ABUSE REPORTING

California Welfare and Institutions Code Section 15659 requires Los Angeles County DPH to provide all "care custodians," "clergy member," "health practioners," and "employees of an adult protective services agency" who enter into employment on or after January 1, 1995, with the following statement prior to commencing his/her employment or assignment and as a prerequisite to that employment or assignment. California law requires this statement to be signed by the workforce member as a prerequisite to employment or assignment and be retained by the Los Angeles County DPH.

Section 15630(b) (1) of the Welfare and Institutions Code provides as follows:

Any mandated reporter who, in his or her professional capacity, or within the scope of his or her employment, has observed or has knowledge of an incident that reasonably appears to be physical abuse, as defined in Section 15610.63 of the Welfare and Institutions Code, abandonment, abduction, Isolation, financial abuse, or neglect, or is told by an elder or dependent adult that he or she has experienced behavior, including an act or omission, constituting physical abuse, as defined in Section 15610.63 of the Welfare and Institutions Code, abandonment, abduction, isolation, financial abuse, or neglect, or reasonably suspects that abuse, shall report the known or suspected instance of abuse by telephone immediately or as soon as practicably possible, and by written report within two working days, either to the long-term care facility, or the either the County adult protective agency or to a local law enforcement agency or other agency that licenses the facility where the physical abuse is alleged to have occurred.

DEFINITIONS

Care Custodian – An administrator or an employee of any of the following public or private facilities or agencies, or persons providing care or services for elders or dependent adults, including members of the support staff and maintenance staff:

a) Twenty-four-hour health facilities, as defined in Sections 1250,1250.2, and 1250.3 of the Health and Safety Code.
b) Clinics
c) Home health agencies
d) Agencies providing publicly funded in-home supportive services, nutrition services, or other home and community-based support services
e) Adult day health care centers and adult day care
f) Secondary schools that serve 18-to-22 year old dependent adults and postsecondary education institutions that serve dependant adults or elders
g) Independent living centers
h) Camps
i) Alzheimer's Disease day care resource centers
j) Community care facilities, as defined in Section 1502 of the Health and Safety Code, and residential care facilities for the elderly, as defined in Section 1569.2 of the Health and Safety Code
k) Respite care facilities
l) Foster homes
m) Vocational rehabilitation facilities and work activity centers
n) Designated area agencies on aging
o) Regional centers for persons with developmental disabilities
p) State Departmental of Social Services and State Department of Health Services licensing divisions
q) County welfare departments
r) Offices of patients' rights advocates and clients' rights advocates, including attorneys
s) The office of the long-term care ombudsman
t) Offices of public conservators, public guardians, and court investigators
u) Any protection or advocacy agency or entity that is designed by the Governor to fulfill the requirements and assurances of the following:
    1) The federal Developmental Disabilities Assistance and Bill of Rights Act of 2000, contained in Chapter 144 (commencing with Section 15001) of Title 42 of the United States Code, for protection and advocacy of the rights of persons with developmental disabilities.
    2) The Protection and Advocacy for the Mentally Ill Individuals Act of 1986, as amended, contained in Chapter 114 (commencing with Section 10801) of Title 42 of the United States Code, for protection and advocacy of the rights of persons with mental illness.
v) Humane societies and animal control agencies
w) Fire departments
x) Offices of environmental health and building code enforcement
y) Any other protective, public, sectarian, mental health, or private assistance or advocacy agency or person providing health services or social services to elders and dependent adults.

Health Practitioner – A physician and surgeon, psychiatrist, psychologist, dentist, resident, intern, podiatrist, chiropractor, licensed nurse, dental hygienist, licensed clinical social worker or associate clinical social worker, marriage, family and child counselor, or any other person who is currently licensed under Division 2 (commencing with Section 500) of the Business and Professions Code, any emergency medical technician I or II, paramedic, or person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code, a psychological assistant registered pursuant to Section 2913 of the Business and Professions Code, a marriage, family and child counselor trainee, as defined in subdivision (c) of section 4980.03 of the Business and Professions Code, or an unlicensed marriage, family, and child counselor intern registered under Section 4980.44 of the Business and Professions Code, state or county public health or social service employee who treats an elder or a dependent adult for any condition, or a coroner.

Dependent Adult – Any person between the ages of 18 and 64 years who resides in this state and who has physical or mental limitations that restrict his or her ability to carry out normal activities or to protect his or her rights, including, but not limited to, persons who have physical or developmental disabilities, or whose physical or mental abilities have diminished because of age.

Dependent adult includes any person between the ages of 18 and 64 years who is admitted as an inpatient to a 24-hour health facilities, as defined in Sections 1250, 1250.2 and 1250.3 of the Health and Safety Code.

Elder – Any person residing in this state, 65 years of age or older.

Abuse – For purposes of elder or dependent adult, "abuse" means (a) physical abuse, neglect, financial abuse, abandonment, isolation, abduction, or other treatment with resulting physical harm or pain or mental suffering, (b) the deprivation by a care custodian of goods or services that are necessary to avoid physical harm or mental suffering.

DOMESTIC/INTIMATE PARTNER VIOLENCE REPORTING

California Penal Code Section 11160 requires any health practitioner employed in a health facility, clinic, physician's office, local or state public health department, or a clinic or other type of facility operated by a local or state public health department who, in his or her professional capacity or within the scope of his or her employment, provides medical services for a physical condition to a patient whom he or she knows or reasonably suspects is a person described as follows, shall immediately, or as soon as practically possible, make a report to local law enforcement by telephone and a written report within two (2) working days of receiving information regarding the person.

- Any person suffering from any wound or other physical injury inflicted by his or her own act or inflicted by another where the injury is by means of a firearm, or
- Any person suffering from any wound or other physical injury inflicted upon the person where the injury is the result of assaultive or abusive conduct.

DEFINITIONS

Assaultive and abusive conduct - includes murder, manslaughter, mayhem, aggravated mayhem, torture, assault with intent to commit mayhem, rape, sodomy, or oral copulation, administering controlled substance or anesthetic to aid in commission of a felony, battery, sexual battery, incest, throwing any vitriol, corrosive acid, or caustic chemical with intent to injure or disfigure, assault with a stun gun or taser, assault with a deadly weapon, firearm, assault weapon, or machinegun, or by means likely to produce great bodily injury, rape, spousal rape, procuring any male/female to have sex with another man/woman, child abuse or endangerment, abuse of spouse or cohabitant, sodomy, lewd and lascivious acts with a child, oral copulation, sexual penetration, elder abuse, an attempt to commit any crime specified above in violation of the California Penal Code.

Domestic Violence (Penal Code 13700)
Abuse committed against an adult or a minor who is a spouse, former spouse, cohabitant, former cohabitant, or person with whom the suspect has had a child or is having or has had a dating or engagement relationship. "Cohabitant" means two (2) unrelated adult persons living together for a substantial period of time, resulting in some permanency of relationship. Factors that may determine whether persons are cohabitating include, but are not limited to, (1) sexual relations between the parties while sharing the same living quarters, (2) sharing of income or expenses, (3) joint use or ownership of property, (4) whether the parties hold themselves out as husband and wife, (5) the continuity of the relationship, and (6) the length of the relationship.

Abuse - Intentionally or recklessly causing or attempting to cause bodily injury, or placing another person in reasonable apprehension of imminent serious bodily injury to himself or herself or another, sexual assault, or engaging in any behavior that has been or could be enjoined pursuant to Section 6320 such as molesting, attacking, striking, stalking, threatening, battering, harassing.

Health Practitioner – A physician and surgeon, psychiatrist, psychologist, dentist, resident, intern, podiatrist, chiropractor, licensed nurse, dental hygienist, licensed clinical social worker or associate clinical social worker, marriage, family and child counselor or any other person who is currently licensed under Division 2 (commencing with Section 500) of the Business and Professions Code, any emergency medical technician I or II, paramedic, or person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code, a psychological assistant registered pursuant to Section 2913 of the Business and Professions Code, a marriage, family and child counselor trainee, as defined in subdivision (c) of Section 4980.03 of the Business and Professions Code, or an unlicensed marriage, family, and child counselor intern registered under Section 4980.44 of the Business and Professions Code, state or county public health or social service employee who treats an elder or a dependent adult for any condition, or a coroner.

Intimate Partner – Intimate partners include current and former spouses (legal and common law), current and former non-marital partners (girlfriend/boyfriend relationship, same-sex partners, dating partners (includes first date).

Intimate Partner Violence – The threatened or actual use of physical force against an intimate partner that either results in or has the potential to result in death, injury, or harm. Intimate partner violence includes physical and sexual violence, both of which are often accompanied by psychological or emotional abuse. It may also include psychological or emotional abuse that occurs without physical or sexual violence when such violence has previously been threatened or committed during the relationship. Some common terms used to describe intimate partner violence include domestic abuse, spouse abuse, domestic violence, courtship violence, battering, marital rape, and date rape. Domestic violence and intimate partner violence are terms used interchangeably.

SEXUAL ABUSE/SEXUAL COERCION/SEXUAL MISCONDUCT (INAPPROPRIATE BEHAVIOR TOWARD A PATIENT)

A workforce member is prohibited from engaging in any conduct of a sexual nature, either intended or unintended, either with or in the presence of any member of the public or patient with whom the workforce member interacts in any way in the performance of his or her work duties. Examples of conduct which may be of a sexual nature include, but are not limited to, verbal, visual, computer generated (e.g., e-mails), written or physical. Sexual misconduct includes inappropriate work-related consensual sexual behavior, whether or not it involves other persons or is done in the presence of other person.

Sexual contact between a health care worker and a patient is strictly prohibited and will constitute sexual misconduct, sexual assault and/or abuse, this includes intercourse as well as touching the patient's body with sexual intent. Unwanted or nonconsensual sexual contact (with or absent of force) involving a patient and another patient, workforce member, unknown perpetrator or spouse/significant other, while being treated or occurring on the premises of a DPH Program may constitute a criminal act punishable by law.

Any workforce member who witnesses or reasonably believes that inappropriate contact and/or sexual assault and/or abuse occurred to a patient must report it to his or her supervisor/head of the department or Administrative officer of the Day (AOD), local law enforcement, the DPH Quality Improvement & Patient Safety, and to the Risk Management hotline (562) 420-5959 following sentinel event reporting procedures.

If the violation involves a County workforce member, the DPH Performance Management unit must also be contacted (323) 890-8466.

DEFINITIONS

Abuse – Intentionally or recklessly causing or attempting to cause bodily injury, or placing another person in reasonable apprehension of imminent serious bodily injury to himself or herself, or another. Sexual abuse includes sexual harassment, sexual coercion and sexual assault (JCAHO).

REPORTING SUSPICIOUS INJURIES

In accordance with California Penal Code Section 11160, DPH requires any health practitioner working in a DPH health facility who is his or her professional capacity or within the scope of his or her assignment provides medical services to a patient who he or she knows or reasonably suspects has a suspicious injury to report such injury by telephone to local law enforcement immediately or as soon as practicable. Section 11160 requires the reporter to make a written follow-up report within two (2) business days to the same local law enforcement agency.

A suspicious injury includes any wound or other physical injury that either was:

- Inflicted by the injured person's own act or by another where the injury was by means of a firearm,
  or
- Is suspected to be the result of assaultive or abusive conduct inflicted upon the injured person.

Health practitioners working in a DPH health facility who are engaged in compiling evidence during a forensic medical examination for a criminal investigation of sexual assault may be asked to release the report to local law enforcement and other agencies, the reports must be prepared on specific forms. Health practitioners must follow DPH HIPPA procedures documenting the release of such information

Section 11165.7 of the Penal Code reads:

11165.7. (a) As used in this article, "mandated reporter" is defined as any of the following:
(1) A teacher.
(2) An instructional aide.
(3) A teacher's aide or teacher's assistant employed by any public or private school.
(4) A classified employee of any public school.
(5) An administrative officer or supervisor of child welfare and attendance, or a certificated pupil personnel employee of any public or private school.
(6) An administrator of a public or private day camp.
(7) An administrator or employee of a public or private youth center, youth recreation program, or youth organization.
(8) An administrator or employee of a public or private organization whose duties require direct contact and supervision of children.
(9) Any employee of a county office of education or the State Department of Education, whose duties bring the employee into contact with children on a regular basis.
(10) A licensee, an administrator, or an employee of a licensed community care or child day care facility.
(11) A Head Start program teacher.
(12) A licensing worker or licensing evaluator employed by a licensing agency as defined in Section 11165.11.
(13) A public assistance worker.
(14) An employee of a child care institution, including, but not limited to, foster parents, group home personnel, and personnel of residential care facilities.
(15) A social worker, probation officer, or parole officer.
(16) An employee of a school district police or security department.
(17) Any person who is an administrator or presenter of, or a counselor in, a child abuse prevention program in any public or private school.
(18) A district attorney investigator, inspector, or local child support agency caseworker unless the investigator, inspector, or caseworker is working with an attorney appointed pursuant to Section 317 of the Welfare and Institutions Code to represent a minor.
(19) A peace officer, as defined in Chapter 4.5 (commencing with Section 830) of Title 3 of Part 2, who is not otherwise described in this section.
(20) A firefighter, except for volunteer firefighters.
(21) A physician, surgeon, psychiatrist, psychologist, dentist, resident, intern, podiatrist, chiropractor, licensed nurse, dental hygienist, optometrist, marriage, family and child counselor, clinical social worker, or any other person who is currently licensed under Division 2 (commencing with Section 500) of the Business and Professions Code.
(22) Any emergency medical technician I or II, paramedic, or other person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code.
(23) A psychological assistant registered pursuant to Section 2913 of the Business and Professions Code.
(24) A marriage, family, and child therapist trainee, as defined in subdivision (c) of Section 4980.03 of the Business and Professions Code.
(25) An unlicensed marriage, family, and child therapist intern registered under Section 4980.44 of the Business and Professions Code.
(26) A state or county public health employee who treats a minor for venereal disease or any other condition.
(27) A coroner.
(28) A medical examiner, or any other person who performs autopsies.
(29) A commercial film and photographic print processor, as specified in subdivision (e) of Section 11166. As used in this article, "commercial film and photographic print processor" means any person who develops exposed photographic film into negatives, slides, or prints, or who makes prints from negatives or slides, for compensation. The term includes any employee of such a person; it does not include a person who develops film or makes prints for a public agency.

(30) A child visitation monitor. As used in this article, "child visitation monitor" means any person who, for financial compensation, acts as monitor of a visit between a child and any other person when the monitoring of that visit has been ordered by a court of law.

(31) An animal control officer or humane society officer. For the purposes of this article, the following terms have the following meanings:

(A) "Animal control officer" means any person employed by a city, county, or city and county for the purpose of enforcing animal control laws or regulations.

(B) "Humane society officer" means any person appointed or employed by a public or private entity as a humane officer who is qualified pursuant to Section 14502 or 14503 of the Corporations Code.

(32) A clergy member, as specified in subdivision (d) of Section 11166. As used in this article, "clergy member" means a priest, minister, rabbi, religious practitioner, or similar functionary of a church, temple, or recognized denomination or organization.

(33) Any custodian of records of a clergy member, as specified in this section and subdivision (d) of Section 11166.

(34) Any employee of any police department, county sheriff's department, county probation department, or county welfare department.

(35) An employee or volunteer of a Court Appointed Special Advocate program, as defined in Rule 1424 of the California Rules of Court.

(36) A custodial officer as defined in Section 831.5.

(37) Any person providing services to a minor child under Section 12300 or 12300.1 of the Welfare and Institutions Code.

(38) An alcohol and drug counselor. As used in this article, an "alcohol and drug counselor" is a person providing counseling, therapy, or other clinical services for a state licensed or certified drug, alcohol, or drug and alcohol treatment program. However, alcohol or drug abuse, or both alcohol and drug abuse, is not in and of itself a sufficient basis for reporting child abuse or neglect.

(b) Except as provided in paragraph (35) of subdivision (a), volunteers of public or private organizations whose duties require direct contact with and supervision of children are not mandated reporters but are encouraged to obtain training in the identification and reporting of child abuse and neglect and are further encouraged to report known or suspected instances of child abuse or neglect to an agency specified in Section 11165.9.

(c) Employers are strongly encouraged to provide their employees who are mandated reporters with training in the duties imposed by this article. This training shall include training in child abuse and neglect identification and training in child abuse and neglect reporting. Whether or not employers provide their employees with training in child abuse and neglect identification and reporting, the employers shall provide their employees who are mandated reporters with the statement required pursuant to subdivision (a) of Section
11166.5.

(d) School districts that do not train their employees specified in subdivision (a) in the duties of mandated reporters under the child abuse reporting laws shall report to the State Department of Education the reasons why this training is not provided.

(e) Unless otherwise specifically provided, the absence of training shall not excuse a mandated reporter from the duties imposed by this article.

(f) Public and private organizations are encouraged to provide their volunteers whose duties require direct contact with and supervision of children with training in the identification and reporting of child abuse and neglect.

Section 11166 of the Penal Code reads:

11166. (a) Except as provided in subdivision (d), and in Section 11166.05, a mandated reporter shall make a report to an agency specified in Section 11165.9 whenever the mandated reporter, in his or her professional capacity or within the scope of his or her employment, has knowledge of or observes a child whom the mandated reporter knows or reasonably suspects has been the victim of child abuse or neglect. The mandated reporter shall make an initial report to the agency immediately or as soon as is practicably possible by telephone and the mandated reporter shall prepare and send, fax, or electronically transmit a written follow-up report thereof within 36 hours of receiving the information concerning the

incident. The mandated reporter may include with the report any non-privileged documentary evidence the mandated reporter possesses relating to the incident.

(1) For the purposes of this article, "reasonable suspicion" means that it is objectively reasonable for a person to entertain a suspicion, based upon facts that could cause a reasonable person in a like position, drawing, when appropriate, on his or her training and experience, to suspect child abuse or neglect. For the purpose of this article, the pregnancy of a minor does not, in and of itself, constitute a basis for a reasonable suspicion of sexual abuse.

(2) The agency shall be notified and a report shall be prepared and sent, faxed, or electronically transmitted even if the child has expired, regardless of whether or not the possible abuse was a factor contributing to the death, and even if suspected child abuse was discovered during an autopsy.

(3) Any report made by a mandated reporter pursuant to this section shall be known as a mandated report.

(b) If after reasonable efforts a mandated reporter is unable to submit an initial report by telephone, he or she shall immediately or as soon as is practicably possible, by fax or electronic transmission, make a one-time automated written report on the form prescribed by the Department of Justice, and shall also be available to respond to a telephone follow-up call by the agency with which he or she filed the report. A mandated reporter who files a one-time automated written report because he or she was unable to submit an initial report by telephone is not required to submit a written follow-up report.

(1) The one-time automated written report form prescribed by the Department of Justice shall be clearly identifiable so that it is not mistaken for a standard written follow-up report. In addition, the automated one-time report shall contain a section that allows the mandated reporter to state the reason the initial telephone call was not able to be completed. The reason for the submission of the one-time automated written report in lieu of the procedure prescribed in subdivision (a) shall be captured in the Child Welfare Services/Case Management System (CWS/CMS). The department shall work with stakeholders to modify reporting forms and the CWS/CMS as is necessary to accommodate the changes enacted by these provisions.

(2) This subdivision shall not become operative until the CWS/CMS is updated to capture the information prescribed in this subdivision.

(3) This subdivision shall become inoperative three years after this subdivision becomes operative or on January 1, 2009, whichever occurs first.

(4) On the inoperative date of these provisions, a report shall be submitted to the counties and the Legislature by the Department of Social Services that reflects the data collected from automated one-time reports indicating the reasons stated as to why the automated one-time report was filed in lieu of the initial telephone report.

(5) Nothing in this section shall supersede the requirement that a mandated reporter first attempt to make a report via telephone, or that agencies specified in Section 11165.9 accept reports from mandated reporters and other persons as required.

(c) Any mandated reporter who fails to report an incident of known or reasonably suspected child abuse or neglect as required by this section is guilty of a misdemeanor punishable by up to six months confinement in a county jail or by a fine of one thousand dollars ($1,000) or by both that imprisonment and fine. If a mandated reporter intentionally conceals his or her failure to report an incident known by the mandated reporter to be abuse or severe neglect under this section, the failure to report is a continuing offense until an agency specified in Section 11165.9 discovers the offense.

(d) (1) A clergy member who acquires knowledge or a reasonable suspicion of child abuse or neglect during a penitential communication is not subject to subdivision (a). For the purposes of this subdivision, "penitential communication" means a communication, intended to be in confidence, including, but not limited to, a sacramental confession, made to a clergy member who, in the course of the discipline or practice of his or her church, denomination, or organization, is authorized or accustomed to hear those communications, and under the discipline, tenets, customs, or practices of his or her church, denomination, or organization, has a duty to keep those communications secret.

(2) Nothing in this subdivision shall be construed to modify or limit a clergy member's duty to report known or suspected child abuse, or neglect when the clergy member is acting in some other capacity that would otherwise make the clergy member a mandated reporter.

(3) (A) On or before January 1, 2004, a clergy member or any custodian of records for the clergy member may report to an agency specified in Section 11165.9 that the clergy member or any custodian of records for the clergy member, prior to January 1, 1997, in his or her professional capacity or within the

scope of his or her employment, other than during a penitential communication, acquired knowledge or had a reasonable suspicion that a child had been the victim of sexual abuse that the clergy member or any custodian of records for the clergy member did not previously report the abuse to an agency specified in Section 11165.9. The provisions of Section 11172 shall apply to all reports made pursuant to this paragraph.

(B) This paragraph shall apply even if the victim of the known or suspected abuse has reached the age of majority by the time the required report is made.

(C) The local law enforcement agency shall have jurisdiction to investigate any report of child abuse made pursuant to this paragraph even if the report is made after the victim has reached the age of majority.

(e) Any commercial film and photographic print processor who has knowledge of or observes, within the scope of his or her professional capacity or employment, any film, photograph, videotape, negative, or slide depicting a child under the age of 16 years engaged in an act of sexual conduct, shall report the instance of suspected child abuse to the law enforcement agency having jurisdiction over the case immediately, or as soon as practicably possible, by telephone and shall prepare and send, fax, or electronically transmit a written report of it with a copy of the film, photograph, videotape, negative, or slide attached within 36 hours of receiving the information concerning the incident. As used in this subdivision, "sexual conduct" means any of the following:

(1) Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex or between humans and animals.

(2) Penetration of the vagina or rectum by any object.

(3) Masturbation for the purpose of sexual stimulation of the viewer.

(4) Sadomasochistic abuse for the purpose of sexual stimulation of the viewer.

(5) Exhibition of the genitals, pubic, or rectal areas of any person for the purpose of sexual stimulation of the viewer.

(f) Any mandated reporter who knows or reasonably suspects that the home or institution in which a child resides is unsuitable for the child because of abuse or neglect of the child shall bring the condition to the attention of the agency to which, and at the same time as, he or she makes a report of the abuse or neglect pursuant to subdivision (a).

(g) Any other person who has knowledge of or observes a child whom he or she knows or reasonably suspects has been a victim of child abuse or neglect may report the known or suspected instance of child abuse or neglect to an agency specified in Section 11165.9. For purposes of this section, "any other person" includes a mandated reporter who acts in his or her private capacity and not in his or her professional capacity or within the scope of his or her employment.

(h) When two or more persons, who are required to report, jointly have knowledge of a known or suspected instance of child abuse or neglect, and when there is agreement among them, the telephone report may be made by a member of the team selected by mutual agreement and a single report may be made and signed by the selected member of the reporting team. Any member who has knowledge that the member designated to report has failed to do so shall thereafter make the report.

(i) (1) The reporting duties under this section are individual, and no supervisor or administrator may impede or inhibit the reporting duties, and no person making a report shall be subject to any sanction for making the report. However, internal procedures to facilitate reporting and apprise supervisors and administrators of reports may be established provided that they are not inconsistent with this article.

(2) The internal procedures shall not require any employee required to make reports pursuant to this article to disclose his or her identity to the employer.

(3) Reporting the information regarding a case of possible child abuse or neglect to an employer, supervisor, school principal, school counselor, coworker, or other person shall not be a substitute for making a mandated report to an agency specified in Section 11165.9.

(j) A county probation or welfare department shall immediately, or as soon as practicably possible, report by telephone, fax, or electronic transmission to the law enforcement agency having jurisdiction over the case, to the agency given the responsibility for investigation of cases under Section 300 of the Welfare and Institutions Code, and to the district attorney's office every known or suspected instance of child abuse or neglect, as defined in Section 11165.6, except acts or omissions coming within subdivision (b) of Section 11165.2, or reports made pursuant to Section 11165.13 based on risk to a child which relates solely to the inability of the parent to provide the child with regular care due to the parent's substance abuse, which shall be reported only to the county welfare or probation department. A county

probation or welfare department also shall send, fax, or electronically transmit a written report thereof within 36 hours of receiving the information concerning the incident to any agency to which it makes a telephone report under this subdivision.

(k) A law enforcement agency shall immediately, or as soon as practicably possible, report by telephone, fax, or electronic transmission to the agency given responsibility for investigation of cases under Section 300 of the Welfare and Institutions Code and to the district attorney's office every known or suspected instance of child abuse or neglect reported to it, except acts or omissions coming within subdivision (b) of Section 11165.2, which shall be reported only to the county welfare or probation department. A law enforcement agency shall report to the county welfare or probation department every known or suspected instance of child abuse or neglect reported to it which is alleged to have occurred as a result of the action of a person responsible for the child's welfare, or as the result of the failure of a person responsible for the child's welfare to adequately protect the minor from abuse when the person responsible for the child's welfare knew or reasonably should have known that the minor was in danger of abuse. A law enforcement agency also shall send, fax, or electronically transmit a written report thereof within 36 hours of receiving the information concerning the incident to any agency to which it makes a telephone report under this subdivision.

COUNTY OF LOS ANGELES
Public Health

County of Los Angeles (County) Volunteer Workers:
Indemnification & Insurance Program Description

Purpose

This handout was developed to provide you, the volunteer, with a brief description of County insurance programs which may be available to you.

Eligibility

To qualify for coverage, you must be formally enrolled as a volunteer in a program or activities sponsored by the County and adhere to established volunteer work assignment guidelines. The County Department to which you are assigned will advise you of your work duties and will maintain an enrollment record to document your participation as a volunteer.

Volunteer Medical Expense Reimbursement Insurance Policy

Purpose

The Volunteer Insurance Policy is intended to reimburse you for *medical expenses associated with the immediate treatment* of an injury you suffer as a result of performing volunteer services, and which are not covered by your own medical insurance. No coverage is provided for injury due to a "personal deviation" while traveling, or for injury contributed to by underlying disease, sickness, mental or bodily infirmity. Volunteers in general are not eligible to receive County workers' compensation benefits.

However, certain designated groups of volunteers may qualify per Board adopted resolutions, California Government Code, or Federal Volunteer Protection Act.

- **Summary of Benefits:**

Volunteers receive medical expense reimbursement and accidental death and dismemberment coverage through a commercial insurance policy purchased by the County. This policy, which is presently written by CIGNA, provides benefits of:

up to $10,000 for accidental medical expenses
up to $500 for accidental dental expenses, and
up to $5,000 for accidental death and dismemberment.

- **Where to Obtain Medical Treatment:**

You may obtain medical treatment from your private physician or other facility of your choice. However, you, the volunteer, are responsible for the initial payment of all medical bills – you must file a claim under the Volunteer Insurance Policy to receive reimbursement from the insurance company for any costs not paid under your own medical insurance.

Volunteers assigned to certain County facilities (such as hospitals) may be able to receive initial treatment at no cost from the County facility in which they work. Your supervisor or volunteer coordinator will advise you of your department's policy regarding provision of initial treatment to volunteers. However, if further medical treatment is deemed necessary, you will be referred to your own private physician and you must file a claim under the Volunteer Insurance Policy to receive reimbursement for your physician's charges.

- **How to Report an Injury, File a Claim and Obtain Reimbursement:**

If you are injured, you must notify your supervisor as soon as possible and assist with the completion of a claim form. In general, instructions for completion of the form require that:

- The volunteer's department supervisor (representative) signs the claim form.
- The volunteer provides certain information including complete name and address, SSN, and a description of the injury. The volunteer is also responsible for ensuring that their treating physician or the treating facility completes the physician's or facility's section of the claim form.
- The volunteer attaches copies of medical bills to the claim form. If medical billings are not readily available, they should be sent as soon as possible to the insurance company.
- The claim form and medical bills should be mailed without delay to CIGNA at the following address:

CIGNA Life & Accident Claim Services
P.O. Box 22328
Pittsburgh, PA 15222-0328

Questions concerning the claim form or the status of your claim may be directed to CIGNA at 1-800-36-CIGNA. Call between 5 am and 5 pm Pacific time and select option 4. If the call falls outside this time frame, leave a voicemail message and a CIGNA representative will respond the next business day.

Another option to file a claim is to call CIGNA's toll-free number and speak with one of the Customer Intake Representatives. CIGNA will take all initial information over the phone at 1-800-36-CIGNA or 1-800-362-4462.

CIGNA will make the final determination to approve or deny your claim in accordance with the terms of the insurance policy.

PLEASE NOTE:

- **Failure to promptly notify your supervisor of injury or late filing of your claim could jeopardize your benefits under this insurance program. If you have another medical insurance plan, it is also important that you notify your insurance company at the same time to preserve your rights to coverage under your own plan.**
- **This brief description of benefits is provided for general informational purposes only, and is not intended to provide all coverage details; the terms, exclusions and conditions concerning the medical benefits are governed by the insurance policy.**
- **Should there be any conflict or inconsistency between the information provided in this handout and the insurance policy, the insurance policy provisions shall prevail.**
- **The County reserves the right to amend or terminate the Volunteer Insurance Policy at any time without notice.**

Third-Party Liability – County Defense and Indemnification of Volunteers and Accident Reporting Procedures

- **Indemnification:**

You are defended and indemnified by the County for professional, auto and general liability (also known as "third party liability), which may arise from your activities as a volunteer within the course of your volunteer assignment, unless your actions are fraudulent, malicious, or criminal. Volunteers are not indemnified for punitive damages. Therefore, it is very important that you have a clear understanding of your work assignment and authority.

- **Volunteers Who Provide Professional Services:**

In the event of any occurrence involving possible injury or death to a County patient or client, you will be required to assist your supervisor in the completion of your department's incident report form. This form may be obtained from your supervisor.

You must report any such incident within 24 hours to your supervisor, even if it did not result in any immediate injury or damage to the patient/client. Fatalities or serious injuries must be reported immediately. The completed incident report will be forwarded by your supervisor to the County's claim administrators.

- **Volunteers Who Drive in the Course of Their Assignment:**

Volunteers who are designated and authorized by the County to operate vehicles in the course and scope of their assignments are defended and indemnified for bodily injury or property damage, suffered by other parties, which may be caused by the volunteer. Such volunteers must possess a valid California driver's license and comply with all California State laws, including laws relating to financial responsibility (automobile liability insurance), seat belts and use of cellular telephones.

You must report any auto accident within 24 hours to your supervisor, even if it did not result in any injury or damage to you or to others. Fatalities or serious injuries must be reported immediately. If the accident caused injury or damage to others, you will be required to assist your supervisor in completing the attached "County of Los Angeles Report of Vehicle Collision or Incident." The completed report will be forwarded by your supervisor to the County's claims administrators. Please note that damage to Volunteer-owned vehicles or loss of personal items is not covered by the County. No coverage is provided for injury due to a "personal deviation" while traveling (for example, if you are injured when driving during your lunch break).

- **All County Volunteers (All Incidents not Involving Professional Liability or Auto Liability):**

Volunteers who witness other types of accidents (such as slips and falls) or who are themselves injured while performing their duties must report any such incident to their supervisors, and assist in completion of the attached "County of Los Angeles Non-Employee Injury Report." Similar to the requirements noted above, fatalities or serious injuries must be reported immediately. Your supervisor will send the completed report to the County's claims administrators.

Please note: Should there be any conflict or inconsistency between the information provided in this handout concerning County defense and indemnification of volunteers and County Code provisions or applicable state law, the County Code and state law shall prevail.

Any questions you may have regarding your volunteer service or this handout may be directed to your supervisor or your department Volunteer Coordinator. The Volunteer Coordinator's for the Department of Public Health is Jessica Mejia, she can be reached at (323) 869-8282.

Prepared By:
County of Los Angeles
Chief Executive Office
Risk Management Branch
3333 Wilshire Blvd., Suite 820
Los Angeles, CA 90010

Effective Date: November 9, 2009

COUNTY OF LOS ANGELES (COUNTY) VOLUNTEER WORKERS: INDEMNIFICATION & INSURANCE PROGRAM DESCRIPTION AND GUIDE

A. Why am I receiving this Guide?

This Guide was developed to provide you, the volunteer, with a brief description of County insurance programs which may be available to you.

B. How do I qualify for these insurance programs?

To qualify for coverage, you must be formally enrolled as a volunteer in a program or activity sponsored by the County and adhere to your volunteer work assignment guidelines. The County Department to which you are assigned will advise you of your work duties and will maintain an enrollment record to document your participation as a volunteer.

C. Am I eligible for any benefits if I am injured while performing my volunteer duties?

The County will reimburse you as a qualified volunteer (see section B of this guide) for *medical expenses associated with the immediate treatment* in case you are injured while performing your assigned volunteer duties, and if you are not covered by your own medical insurance including personal, group, blanket, employee, trustee, or union insurance plans.

1. What Benefits Will I Receive?

Volunteers receive medical expense reimbursement and accidental death and dismemberment coverage through a commercial insurance policy purchased by the County. This policy, which is presently written by Ace American Insurance Company (Ace), provides benefits of:

(a) Up to $10,000 for accidental medical expenses. An emergency evacuation benefit may be available if the volunteer is severely injured while traveling 100 miles or more away from his home to perform assigned volunteer duties for the County.
(b) Up to $500 for accidental dental expenses.
(c) Up to $5,000 for accidental death and dismemberment.

Ace will make the final determination to approve or deny your claim in accordance with the terms of the insurance policy.

2. Where Do I Go to Obtain Medical Treatment if I am injured?

You may obtain medical treatment from your private physician or other facility of your choice. However, you, the volunteer, are responsible for the initial payment of all medical bills – you must file a claim under the Volunteer Insurance Policy to receive reimbursement from the insurance company for any costs not paid under your own medical insurance.

Volunteers assigned to certain County facilities (such as hospitals) may be able to receive initial treatment at no cost from the County facility in which they work. Your supervisor or volunteer coordinator will advise you of your department's policy regarding provision of initial treatment to volunteers. However, if further medical treatment is deemed necessary, you will be referred to your own private physician and you must file a claim under the Volunteer Insurance Policy to receive reimbursement for your physician's charges.

3. How Do I Report an Injury, File a Claim and Obtain Reimbursement?

If you are injured, you must notify your supervisor as soon as possible and assist with the completion of a claim form. In general, instructions for completion of the form require that:

- The volunteer's department supervisor (representative) signs the claim form.
- The volunteer provides certain information including complete name, address, SSN, date of birth, contact information and a description of the injury. The volunteer is also responsible for ensuring that their treating physician or the treating facility completes the physician's or facility's section of the claim form.
- The volunteer attaches copies of medical bills to the claim form. If medical billings are not readily available, they should be sent to Health Special Risk Inc. (HSR) as soon as possible.
- The signed claim form and medical bills should be faxed (preferred option) OR mailed without delay to HSR:

Fax line:	972-512-5820
	-OR-
Mailing Address:	Health Special Risk, Inc. (HSR) 4100 Medical Parkway Carrollton, Texas 75007
	-OR-
Email:	ACEClaims@hsri.com

- You also may initiate a claim by calling HSR Customer Intake Representative who will take your initial information over the phone at 866-345-0959.
- The claim is assigned to a designated Accident Claims Specialist who may contact you if additional information is needed. If necessary, the Claim Specialist will generate an acknowledgement package to send to you or your beneficiary. You or

your beneficiary will complete your portion of the claim form and send it back.

4. How Can I Check the Status of My Claim with CIGNA?

Questions concerning the claim form or the status of your claim may be directed to HSR at 1-866-345-0959. Call between 5 am and 5 pm Pacific Time and select option 4. If you call outside this time frame, leave a voicemail message and a CIGNA representative will respond the next business day.

PLEASE NOTE: This brief description of benefits is provided for general informational purposes only, and is not intended to provide all coverage details; the terms, exclusions and conditions concerning the medical benefits are governed by the insurance policy. Should there be any conflict or inconsistency between the information provided in this guide and the insurance policy, the insurance policy provisions shall prevail. The County reserves the right to amend or terminate the Volunteer Insurance Policy at any time without notice.

D. Will I be protected against liability if I should accidentally cause harm to someone while performing my assigned volunteer duties?

You are defended and indemnified by the County for professional, auto and general liability (also known as "third party liability), which may arise from your activities as a volunteer within the course of your volunteer assignment, unless your actions are fraudulent, malicious, or criminal. Volunteers are not indemnified for punitive damages. Therefore, it is very important that you have a clear understanding of your work assignment and authority.

Reporting requirements: You must report any incident you witnessed or you were involved in while performing your assigned volunteer duties within 24 hours to your supervisor, even if the incident did not result in any immediate injury or damage to anyone. Fatalities or serious injuries must be reported immediately. The completed incident report will be forwarded by your supervisor to the County's claim administrators.

1. Will I Be Protected If I Provide Professional Services As a Volunteer?

In the event of any occurrence involving possible injury or death to a County patient or client, you will be required to assist your supervisor in the completion of your department's incident report form. This form may be obtained from your supervisor (see the reporting requirements noted above).

2. Will I Be Protected If I am Involved in Motor Vehicle Accident While Driving in the Course of My Volunteer Assignment?

Volunteers who are designated and authorized by the County to operate vehicles in the course and scope of their assignments are defended and indemnified for bodily injury or property damage, suffered by other parties, which may be caused by the

volunteer. Such volunteers must possess a valid California driver's license and comply with all California State laws, including laws relating to financial responsibility (automobile liability insurance), seat belts and use of cellular telephones.

In addition to the reporting requirements noted above, you will be required to assist your supervisor in completing the attached "County of Los Angeles Report of Vehicle Collision or Incident" if the accident caused injury or damage to others. Please note that damage to Volunteer-owned vehicles or loss of personal items is not covered by the County. No coverage is provided for injury due to a "personal deviation" while traveling (for example, if you are injured when driving during your lunch break). County encourages you to avoid driving as much as possible while performing your volunteer assignment.

3. If There Is an Incident not Involving Professional or Auto Liability:

In addition to the reporting requirements noted above, you will be required to assist your supervisor in completing the attached "County of Los Angeles Non-Employee Injury Report" if you witness other types of accidents (such as slips and falls) or if you are injured while performing your duties.

Please note: Should there be any conflict or inconsistency between the information provided in this handout concerning County defense and indemnification of volunteers and County Code provisions or applicable state law, the County Code and state law shall prevail.

Any questions you may have regarding your volunteer service or this guide may be directed to your supervisor or your department Volunteer Coordinator. The Volunteer Coordinator's name and telephone number may be obtained from your supervisor.

Prepared By:
County of Los Angeles
Chief Executive Office
Risk Management Branch
3333 Wilshire Blvd., Suite 820
Los Angeles, CA 90010

Effective Date: January, 2010

ATTACHMENT I

OFFICE OF SECURITY MANAGEMENT / CHIEF ADMINISTRATIVE OFFICE
SECURITY INCIDENT REPORT

This report should be completed by the person reporting or involved in the incident, the building manager or his/her designee no later than the end of the business day following the incident. The report shall be delivered to the Office of Security Management, 785 Kenneth Hahn Hall of Administration, 500 West Temple Street, Los Angeles, California 90012, or send FAX (213) 613-0848.

For this report, a SECURITY INCIDENT is defined as:

An incident placing a person or property at risk that requires action by law enforcement authorities, County Office of Public Safety Policy or security guards at a County facility whether they were summoned or not, OR,

An incident placing a person at risk of involving an ON-DUTY County employee (including lunch periods) while on County property. This classification includes parking facilities, or while walking to or from an off-site parking facility to start or end a work day, OR,

An incident of a suspicious or unusual nature on County Property that places people or property at risk.

DATE OCCURRED: _____ DAY OF WEEK: _____ TIME: _____

COUNTY DEPT. REPORTING INCIDENT: _____

ADDRESS OF INCIDENT: _____

Is the suspect a County Employee? Yes ( ) No ( )
Is this incident gang related? Yes ( ) No ( )
Was an arrest made? Yes ( ) No ( )
Charge: _____

The law enforcement agency that handled the incident: (Circle appropriate number)

	Department.	Report Number
1.	L. A. Sheriff's Department	_____
2.	L. A. Police Department	_____
3.	Local Police Department	_____
4.	L. A. County Police	_____
5.	Contract Security Co.	_____
6.	None	_____

CODE FOR TYPE OF INCIDENT REPORTED: _____ (Refer to next page)
(i.e., A-1 = Burglary of a County Building)

REPORTED BY: _____ Daytime Phone: _____

APPROVED BY: _____ Daytime Phone _____

ONLY ATTACH REPORTS AND MATERIALS PERTAINING TO INCIDENTS OF THREATS AND VIOLENCE. ALL OTHER REPORTS AND INFORMATION SHOULD BE FORWARDED TO APPROPRIATE PERSONNEL AND FILED FOR FUTURE REFERENCE.

This form is to be completed in addition to other reports required per County policy or State or Federal laws and regulations.
Distribution: Office of Security Management (Original); Department Head; Departmental Human Resources;

CODE REFERENCE SHEET FOR SECURITY INCIDENT REPORTS

A. Burglary: **Entering a *closed* building or *locked* vehicle with the intent to commit a theft. (459 P.C.)**

1. Burglary of a County building
2. Burglary of a County vehicle
3. Burglary of a Private vehicle
4. Burglary Alarm – no evidence of any crime.

B. Robbery: **The taking of property by force or fear. (211 P.C.)**

1. Robbery of a County facility or employees performing their job.
2. Robbery of a person, including employees, ***not*** performing their job.

C. Arson: **The intentional setting fire to any object. Not necessary to destroy the object. The mere charring is sufficient for arson.**

1. Arson of a County building (447 P.C.)
2. Arson of a County vehicle (447 P.C.)
3. Arson of private property (including vehicles) (447 P.C.)

D. Rape: **Forced sexual intercourse with the opposite sex. (261 P.C.)**

1. Rape of a County employee
2. Rape of other than a County employee
3. Other sex related incident

E. Assault: **The physical battering of another person.**

1. Assault with a weapon (245 P.C.)
2. Assault no weapon but requiring hospitalization of the victim (245 P.C.)
3. Assault with only minor injuries and no weapon was used (245 P.C.)

F. Theft of or from a vehicle:

1. Theft of a County vehicle (487.3 P.C.)
2. Theft of a Private vehicle (487.3 P.C.)
3. Theft from a County vehicle – no forced entry (488 / 487 P.C.)
4. Theft from a Private vehicle – no forced entry (488 / 487 P.C.)

G. Theft not involving a vehicle:

1. Theft of County property valued under $400.00 (488 P.C.)
2. Theft of County property valued over $400.00 (488 P.C.)
3. Theft of private property (excluding vehicles) (488 / 487 P.C.)

H. Disturbances: **No actual crime need be committed. The disruption of routine business constitutes a disturbance.**

1. Disturbance of a County employee or facility (415 P.C.)
2. Disturbance created by a County employee and/or their spouse involving a "domestic issue."
3. Disturbance not involving County employees
4. Threats (verbal or written) to a County employee (422 P.C.)
5. Refusal to be searched.

I. Vandalism: **This classification includes all forms of intentional damage to property and vehicles except arson (refer to "C").**

1. Vandalism to County property, except vehicles (594 P.C.)
2. Vandalism to Private property, except vehicles (594 P.C.)
3. Vandalism to County vehicles (594 P.C.)
4. Vandalism to Private vehicles (594 P.C.)

J. Miscellaneous: **Crimes/activities not covered in any of the above classifications.**

1. Suspicious activity by a non-County employee
2. Suspicious activity by a County employee (explain activity)
3. Hostage situation
4. Bomb threat
5. Suspicious package/substance
6. Bomb or explosive device actually found
7. Power failure
8. Equipment failure
9. Other activity not covered in any other classification (explain in detail) (Lost/stolen badges, bioterrorism activity, hazardous release,etc.)

K. Person sick or injured/mental not the result of criminal activity:

1. Rescue responded
2. Person sent to hospital
3. First aid given by other than Rescue personnel
4. Handled by Security personnel
5. Person refused treatment
6. Other (specify)
   (Hazardous exposure, etc.)

L. Confiscation of contraband:

1. Weapon (gun, knife, club, etc.)
2. Narcotics (any non-prescription drug)
3. Other (specify)

M. *FOR USE BY COURTS ONLY:*

1. Restraints used
2. Escape
3. Attempted escape
4. Physical altercation within a Court facility
5. High risk trial
6. Threats (verbal or written) to a judge
7. Threats (verbal or written) to a jury
8. Attempted unlawful entry