



County of Los Angeles
**CHIEF EXECUTIVE OFFICE
OPERATIONS CLUSTER**

WILLIAM T FUJIOKA
Chief Executive Officer

DATE: August 8, 2013
TIME: 1:00 p.m.
LOCATION: Kenneth Hahn Hall of Administration, Room 830

AGENDA

Members of the Public may address the Operations Cluster on any agenda item by submitting a written request prior to the meeting.
Three (3) minutes are allowed for each item.

1. Call to order – Gevork Simdjian
- A) **Board Letter – RECOMMENDATION TO APPROVE AMENDMENT NO. SIX TO THE ELECTION SYSTEMS AND SOFTWARE, LLC CONTRACT NO. 73635**
RR/CC – Dean Logan or designee
- B) **2012-13 Civil Grand Jury Final Report Responses**
CEO – Frank Cheng or designee
- C) **Review of IT Board Policies No. 6.100 through 6.112**
CIO – Richard Sanchez or designee
- D) **Management Fellows Program Update**
DHR – Lisa Garrett or designee
2. Public Comment
3. Adjournment



DEAN C. LOGAN
Registrar-Recorder/County Clerk

August 20, 2013

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, California 90012

Dear Supervisors:

**RECOMMENDATION TO APPROVE AMENDMENT NUMBER SIX TO THE
ELECTION SYSTEMS AND SOFTWARE, LLC CONTRACT NUMBER 73635
(ALL SUPERVISORIAL DISTRICTS) (3 VOTES)**

SUBJECT

The Los Angeles County Registrar-Recorder/County Clerk (RR/CC) seeks to execute a contract amendment with Election Systems and Software, LLC (ESS) to exercise the last one-year option extension and six one-month option periods concurrently, effective September 1, 2013 through February 28, 2015 in exchange for providing Absentee Voter (Vote-by-Mail) ballot material processing services at a reduced cost.

IT IS RECOMMENDED THAT YOUR BOARD:

1. Delegate authority to the Director of the RR/CC, or designee to execute an amendment (substantially similar to the attached amendment) to the ESS Contract Number 73635, provided that County Counsel approval is obtained prior to initiating any such action. The contracts current option term expires on August 31, 2013. Under Amendment Number Six, the last one-year option extension and six month-to-month option extensions will be exercised concurrently, effective September 1, 2013 through February 28, 2015 in exchange for a reduction in costs.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION:

The current option extension began on September 1, 2012, and expires on August 31, 2013. The purpose of the recommended actions will enable the Contractor to continue providing critical automated Vote-by-Mail ballot processing services for all scheduled and special elections for the remainder of the option terms, effective September 1, 2013 through February 28, 2015 in exchange for a reduced cost.

Under the contract's current payment structure, the RR/CC's costs rise as the number of voters opting to vote by mail in Los Angeles County increases. In an effort to reduce costs, the RR/CC approached the Contractor and proposed modifying the current payment structure from a per-service-fee to a flat fee. Currently, ESS charges a total of \$0.25 per envelope resulting in a variance in cost due to the number of envelopes processed per election. From 2002 to 2012 the number of registered permanent Vote-by-Mail voters has increased from approximately 157,000 to 1.2 million, an increase of 764 percent.

ESS agreed to provide a flat fee for processing ballot return envelopes (incoming mail process) , which resulted in significant savings to the County, in exchange for exercising the last one-year option and six month-to-month option extensions, for a total of 18 months. The Contractor's offer includes transitioning from a per-service-fee to a flat fee **plus** a continuation of the six (6) percent contract cost reduction currently in effect. The flat fee will place a spending cap on costs. This effort will generate a minimum estimated Net County Cost (NCC) savings of approximately \$200,000. The cost savings are a result of (1) changing payment structure from a per-service-fee to a flat fee as related to services provided during the incoming Vote-by-Mail ballot process and; (2) extending the six (6) percent discount that was initially implemented through the Contract Extension/Cost Reduction initiative that would have otherwise expired on August 31, 2013.

The extension will allow the Contractor to continue to perform critical election operations without an interruption in services at a substantially reduced cost.

Implementation of Strategic Plan Goals

This request supports the County Strategic Plan Goals No. 1: Operational Effectiveness: "Maximize the effectiveness of processes, structure, and operations to support timely delivery of customer-oriented and efficient public services" and No. 2: Fiscal Sustainability: "Strengthen and enhance the County's capacity to sustain essential County services through proactive and prudent fiscal policies and stewardship."

FISCAL IMPACT/FINANCING:

Modifications to the payment structure will save the County approximately \$200,000 during the last one-year option period and six month-to-month option extensions. These savings impact the County positively since this Agreement is funded in its entirety by Net County Cost funds.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS:

The RR/CC is responsible for registering voters and maintaining voter files; conducting federal, state, local and special elections; and verifying initiatives, referendums, and recall petitions. With more than 500 political districts and 4.3 million registered voters, the County is the largest and most complex election jurisdiction in the nation. Pursuant to the California Elections Code Section 3201, any registered voters can Vote-by-Mail.

The Agreement with ESS (Formerly Global Elections Systems, Diebold, and Premier) was executed on September 4, 2001. Since then, various contract change notices and Amendments have been granted to either enhance the scanning and mailing system to comply with changes in the regulatory environment, reduce costs, or make necessary modifications to the Agreement to up-date pertinent information as requested by either the County or the Contractor. Additionally, the County has extended the initial term and exercised option extensions. At this time, a total of 18 months of option terms remain on the contract.

CONTRACTING PROCESS:

Pursuant to this Amendment, the department will exercise the last one-year option and six month-to-month option extensions, which will extend this Agreement until February 28, 2015.

CONTRACTOR PERFORMANCE:

The Contractor has met contract performance standards to recommend the extension.

IMPACT ON CURRENT SERVICES:

Los Angeles County processes more Vote-by-Mail ballots than any other county in California. Approval of this extension will result in a substantial savings to the County as we continue mission critical services and provide the necessary resources for processing the high volume of Vote-by-Mail ballots that enable the County to meet functional, business and legal requirements mandated by Federal and State laws.

During the extension period, the Contractor will provide automated Vote-by-Mail processing services for the following elections: (1) UDEL on November 5, 2013; (2) Statewide Primary on June 3, 2014; (3) Statewide General on November 4, 2014 and; (4) Special elections, to be determined.

CONCLUSION:

Approval of delegated authority to the Registrar-Recorder/County Clerk to extend this Agreement for the last one-year option period and six month-to-month option extensions will lock in significant savings and continue to provide election critical services to the residents of the County.

Respectfully submitted,

Dean C. Logan
Registrar-Recorder/County Clerk

DCL:APL:PT
FEP:ca

Attachments

c: Chief Executive Office
County Counsel
CIO

**AMENDMENT NUMBER SIX
TO AGREEMENT 73635
WITH
ELECTION SYSTEMS & SOFTWARE, LLC
FOR
ABSENTEE VOTER BALLOT MATERIAL PROCESSING**

AMENDMENT NUMBER SIX

**TO AGREEMENT 73635
WITH ELECTION SYSTEMS AND SOFTWARE, LLC
FOR ABSENTEE VOTER BALLOT MATERIAL PROCESSING**

This Amendment Number Six ("Amendment Number Six") to Agreement Number 73635 ("Agreement") is entered into this _____ day of _____, 2013 by and between County of Los Angeles, a political subdivision of the State of California ("County") and Election Systems and Software, LLC. ("Contractor"). County and Contractor are sometimes hereinafter referred to collectively as the "Parties" and each individually as a "Party."

WHEREAS, the Agreement was originally entered into by and between County and Global Election Systems, Inc. ("Global") and approved by the County's Board of Supervisors on September 4, 2001;

WHEREAS, under that certain Change Notice Number One to the Agreement dated January 22, 2002, the Agreement was amended to reflect, among other things, a change in the identity of Contractor's Project Manager;

WHEREAS, under that certain Change Notice Number Two to the Agreement dated January 29, 2002, the Agreement was further amended to, among other things, approve subcontracting of the inserting process of the Absentee Voter Ballot Material processing;

WHEREAS, under that certain Change Notice Number Three to the Agreement dated August 8, 2003, the Agreement was further amended to reflect, among other things, (i) the acquisition of Global by Diebold Elections Systems, Inc. and (ii) a further change in the identity of Contractor's Project Manager;

WHEREAS, under that certain Change Notice Number Four to the Agreement dated February 18, 2004, the Agreement was further amended to reflect, among other things, a further change in the identity of Contractor's Project Manager;

WHEREAS, under that certain letter from County to Contractor dated August 18, 2004, County exercised its option to extend the term of the Agreement for a six-month period from September 5, 2004 through March 4, 2005;

WHEREAS, under that certain Change Notice Number Six to the Agreement dated January 19, 2005, County exercised its option to further extend the term of the Agreement for an additional ninety (90) day period from March 5, 2005 through June 2, 2005;

WHEREAS, under that certain Amendment Number One to the Agreement dated June 2, 2005, the Agreement was further amended to, among other things, (i) replace Exhibit A (Statement of Work) with a new Exhibit A1 (Statement of Work) (Amended June 2, 2005) and; (ii) further extend the term of the Agreement for one-year period from June 3, 2005 through June 2, 2006;

WHEREAS, under that certain Change Notice Number Seven to the Agreement dated April 7, 2006, the Agreement was further amended to, among other things, (i) replace Exhibit A1

(Statement of Work) (Amended June 2, 2005) with a new Exhibit A1 (Statement of Work) (Amended April 7, 2006), and; (ii) replace Exhibit B (Price Matrix) with a new Exhibit B (Price Matrix) (Revised October 19, 2005);

WHEREAS, under that certain Change Notice Number Eight to the Agreement dated May 1, 2006, County exercised its option to further extend the term of the Agreement for an additional one-year period from June 3, 2006 through June 2, 2007;

WHEREAS, under that certain Change Notice Number Nine to the Agreement dated March 12, 2007, County exercised its option to further extend the term of the Agreement for an additional 90-day period from June 3, 2007 through August 31, 2007;

WHEREAS, under that certain Amendment Number Two dated July 31, 2007 the Agreement was further amended to, among other things, (i) extend the term of the Agreement for an additional three-year period commencing September 1, 2007 through August 31, 2010, (ii) provide County with options to further extend the term of the Agreement for two (2) one-year periods and six (6) month-to-month periods; (iii) increase the Contract Sum by \$3,864,000; (iv) replace the current Exhibit A1 (Statement of Work (Amended April 7, 2006)) with a new Exhibit A1 (Statement of Work) (Amended September 1, 2007); and (v) replace the current Exhibit B (Price Matrix (Revised June 1, 2006)) with a new Exhibit B (Price Matrix (Revised September 1, 2007));

WHEREAS, under that certain Change Notice Number Ten to the Agreement dated September 6, 2007, County amended the Agreement to recognize the corporate name change for Premier Election Solutions;

WHEREAS, under that certain Change Notice Number Eleven to the Agreement dated April 17, 2008, County amended the Agreement to, among other things, (i) incorporate the requirements and cost of modified return envelopes and provide for any urgent additional orders, (ii) replace the current Exhibit B (Price Matrix (Revised September 1, 2007)) with a new Exhibit B (Price Matrix (Revised March 6, 2008));

WHEREAS, under that certain Amendment Number Three dated October 23, 2009, pursuant to the Board of Supervisors approval of the Contract Extension/Cost Reductions initiative, the Agreement was further amended to, among other things, (i) extend the Initial Term of the Agreement for an additional two-year period thereby extending the base contract coverage period to August 31, 2012, (ii) increase the Contract Sum by \$5,000,000 to account for the term extension; (iii) replace the current Exhibit B (Price Matrix (Revised March 6, 2008)) with a new Exhibit B (Price Matrix) (Revised September 15, 2009);

WHEREAS, under that certain Change Notice Number Twelve to the Agreement dated February 3, 2010, the Agreement was further amended to, recognize the purchase of Premier Election Solutions from Diebold to Election Systems & Software;

WHEREAS, under that certain Amendment Number Four dated August 2, 2011, the Agreement was further amended to, among other things, (i) exercise the first option year

extension with a continuation of the 6% price reduction which originated under the Board's Contract Extension/Price Reduction Program; (ii) exercise the authority granted to the Registrar-Recorder/County Clerk to increase the Contract Sum by 20% or One Million Seven Hundred and Seventy Two Thousand Eight Hundred Dollars (\$1,772,800); (iii) change the identity of County's Project Director; (iv) change the identity of County's Project Manager; (v) change the identity of County's Project Monitor; (vi) replace the current Exhibit A1 (Statement of Work) (Amended September 1, 2007) with a new Exhibit A1 (Statement of Work) (Amended July 1, 2011); and (vii) replace the current Exhibit B (Price Matrix (Revised September 15, 2009)) with a new Exhibit B (Price Matrix (Revised July 1, 2011));

WHEREAS, under that certain Amendment Number Five dated January 25, 2012 the Agreement was further amended to, among other things, (i) recognize the merger of Premier Election Solutions, Inc. with and into Election Systems & Software, Inc; and (ii) recognize the restructuring of Election Systems & Software, Inc. to a limited liability company, Election Systems & Software, LLC;

WHEREAS, the County and Contractor wish to further amend the Agreement to, among other things, (i) exercise the last option year extension and six (6) month-to-month option periods effective September 1, 2013 through February 28, 2015 (ii) continue the six (6) percent price reduction which originated under the Board's Contract Extension/Price Reduction Initiative; (iii) replace Paragraph 12.1 (Indemnification) with a new Paragraph 12.1 (Indemnification); (iv) replace Paragraph 6.0 (Term), subparagraph 6.4, with a new Paragraph 6.0 (Term), subparagraph 6.4; and (v) replace the current Exhibit B (Price Matrix (Revised July 1, 2011)) with a new Exhibit B (Price Matrix (Revised September 1, 2013)) to reflect the transition from a per-service-fee to a flat fee; (vi) add Paragraph 52.0 (Guidelines for Media Sanitation); and

WHEREAS, this Amendment Number Six is made pursuant to Paragraph 4.0 (Change Notices and Amendments) of the Agreement.

NOW THEREFORE, in consideration of the foregoing and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Agreement, as previously amended, is hereby further amended as follows:

1. Pursuant to Paragraph 6.0 (Term), Paragraphs 6.2 and 6.4 of the Agreement, County hereby exercises its authority to extend the Agreement for all remaining option periods, including the last "Extension Year" and six (6) month-to-month option periods, effective from September 1, 2013 through February 28, 2015.
2. Continues the six (6) percent price reduction which originated pursuant to the Board of Supervisor's Contract Extension/Price Reduction Initiative pursuant to Amendment Number Three dated October 23, 2009.
3. Paragraph 6.0 (Term), subparagraph 6.4, of the Agreement is hereby deleted in its entirety and shall be replaced by a new Paragraph 6.0 (Term), subparagraph 6.4, to read as follows:

6.4 County further authorizes Registrar-Recorder/County Clerk, or his designee, at his or her discretion, to authorize additional month-to-month extensions of the Term for a period not to exceed six (6) months, at the end of the initial Term or each Extension year, if exercised. Contractor agrees that such extension(s) shall be at the rate (s), terms and conditions in accordance with Exhibit B.

4. Paragraph 12.1 (Indemnification), of the Agreement is hereby deleted in its entirety and shall be replaced by a new Paragraph 12.1 (Indemnification), to read as follows:

12.1 INDEMNIFICATION

The Contractor shall indemnify, defend and hold harmless the County, its Special Districts, elected and appointed officers, employees, agents and volunteers ("County Indemnitees") from and against any and all liability, including but not limited to demands, claims, actions, fees, costs and expenses (including attorney and expert witness fees), arising from and/or relating to this Contract, except for such loss or damage arising from the sole negligence or willful misconduct of the County Indemnitees.

5. Exhibit B (Price Matrix) (Revised July 1, 2011) of the Agreement is hereby deleted in its entirety and shall be replaced with a new Exhibit B (Price Matrix) (Revised September 1, 2013), a true and correct copy of which is attached hereto and incorporated herein by this reference.

6. Adds a new Paragraph 52.0 (Guidelines for Media Sanitation) to the Agreement to read as follows:

52.0 GUIDELINES FOR MEDIA SANITATION

Contractor(s) and Vendor(s) that have maintained, processed, or stored the County of Los Angeles' ("County") data and/or information, implied or expressed, have the sole responsibility to certify that the data and information have been appropriately destroyed consistent with the National Institute of Standards and Technology (NIST) Special Publication SP 800-88 titled Guidelines for Media Sanitization.

Available at:<http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-88-Rev.%201>

The data and/or information may be stored on purchased, leased, or rented electronic storage equipment (e.g., printers, hard drives) and electronic devices (e.g., servers, workstations) that are geographically located within the County, or external to the County's boundaries.

The County must receive within ten (10) business days, a signed document from Contractor(s) and Vendor(s) that certifies and validates the data and information were placed in one or more of the following stored states: unusable, unreadable, and indecipherable.

Vendor shall certify that any County data stored on purchased, leased, or rented electronic storage equipment and electronic devices, including, but not limited to printers, hard drives, servers, and/or workstations are destroyed consistent with the current National Institute of Standard and Technology (NIST) Special Publication SP-800-88, Guidelines for Media Sanitization. Vendor shall provide County with written certification, within ten (10) business days of removal of any electronic storage equipment and devices that validates that any and all County data was destroyed and is unusable, unreadable, and or undecipherable.

7. Except as otherwise provided under this Amendment Number Six, the Agreement, as previously amended, and including all preambles and recitals set forth herein and therein, shall remain unchanged and in full force and effect.

Draft

**AMENDMENT NUMBER SIX
TO AGREEMENT 73635
WITH PREMIER ELECTION SOLUTIONS
FOR ABSENTEE VOTER BALLOT MATERIAL PROCESSING**

IN WITNESS WHEREOF, the Board of Supervisors of the County of Los Angeles has caused this Amendment Number Six to be subscribed on its behalf by the Registrar-Recorder/County Clerk or his/her designee and the Contractor has subscribed the same through its duly authorized officer as of the day, month and year first above written. The persons signing on behalf of Contractor warrant under penalty of perjury that he or she is authorized to bind the Contractor.

COUNTY OF LOS ANGELES

DEAN C. LOGAN
Registrar-Recorder/County Clerk

ELECTION SYSTEMS & SOFTWARE, LLC

AUTHORIZED SIGNATURE

PRINT OR TYPE NAME

TITLE

Tax Identification Number

APPROVED AS TO FORM:

JOHN F. KRATTLI
County Counsel

By _____
Brandi Miles Moore
Senior Deputy County Counsel

**ABSENTEE VOTER BALLOT MATERIAL PROCESSING
PRICE MATRIX**

(Amended September 1, 2013)

The billing components of the Agreement shall consist of six (6) major components: Materials, Outgoing Mail, Incoming Mail, Automated Signature Recognition (ASR), Miscellaneous Services, and Reduction/Discount. The unit price for each component shall be based on actual materials and/or services performed. Price shall include any and all charges including shipping and delivery cost and all applicable taxes. Contractor shall invoice County for materials provided and services performed in accordance with this Price Matrix.

1. MATERIALS:

1. Outgoing Window Envelopes:
 - a. First Class
 - b. Federal Frank (Military/Overseas) Indicia
 - c. Blank Indicia for Metering
 - d. Non Profit
2. Return Envelopes
 - a. Courtesy Reply
 - b. Business Reply Conforming to Qualified Business Reply Mail (QBRM) Standards
 - c. Federal Frank – Military
 - d. Federal Frank – Overseas

2. OUTGOING MAIL PROCESS: The unit price shall include but is not limited to the following processes:

1. Voter data extract processing, bar coding and inkjet printing of voter specific variable data on the custom ballot return envelope.
2. On demand envelope printing per voter. VoteRemote and Counter software used for distribution of ballots to voters.
3. Automated inserting of absentee ballot materials per Road Maps (15+ groups).
4. Automated sorting of absentee ballot materials by postal Sectional Center Facility (SCF).
5. On-Site Project Management.

3. INCOMING MAIL PROCESS: SCHEDULED ELECTIONS AND SPECIAL ELECTIONS: The flat fee unit price shall include but is not limited to the following processes:

1. Basic Data Capture to support the Voter Signature Verification return database containing the VIMS Absentee Voter Identification Number specified order or group in a tray. This database is delivered to RR/CC on electronic media.
2. VoteRemote Signature Capture which supports item #1 above plus provides additional data elements consisting of signature clips associated with the tray envelopes. The form of the data will be compressed TIFF files named with the Absentee Voter identification.
3. Automated Signature Recognition ("ASR") is a specialized computer software program that compares signatures on absentee ballot with registered voter signature on file.
4. RR/CC will provide Contractor with a written report of its use of ASR within 30 days of each Election. Contractor will invoice County based on the attached pricing structure.

4. AUTOMATED SIGNATURE RECOGNITION SET-UP:

Contractor shall install ASR capability on one or more computers at the RR/CC Headquarters facility in Norwalk for use by or at the direction of Contractor to provide services to County. ASR will run on a dedicated PC with enough licenses to account for the county's volume over each 12 month period. Pricing per license based on attached pricing structure.

5. MISCELLANEOUS TIME AND MATERIALS CHARGE, EMERGENCY/RUSH ORDERS

1. An hourly rate for non-scheduled services (processing, maintenance, etc.) as requested and agreed to by the RR/CC.
2. A per piece rate for non-scheduled emergency/rush envelope orders as requested and agreed to by the RR/CC. Price includes custom USPS approved envelope and any product modifications.
3. Due to unforeseen special circumstances, there may become a need for special products or services that are crucial to the success of an election. If such a determination is made by Registrar-Recorder/County Clerk or designee, Contractor shall provide RR/CC with a cost estimate for review and approval. No such product or service shall be provided by Contractor without written approval of Registrar-Recorder/County Clerk or designee. At no time shall the cost of the product or service in conjunction with other VBM services provided in the Agreement exceed the maximum contract sum approved by the Board of Supervisors.

6. REDUCTION/DISCOUNT

1. Extend the current six percent (6%) pre-tax cost reduction currently in place, for the contract extension effective September 1, 2013 through February, 28, 2015.

Exhibit B

All invoices shall reference each component and specific description category as referenced herein:

	COMPONENT NO.	DESCRIPTION	UNIT PRICE
1	Materials	a. Custom USPS approved, windowed envelope b. Custom USPS approved, punched hole, flood coated, Reply envelope	\$0.06 \$0.055
2	Outgoing Mail Process	a. VoteRemote Software & Management b. Ink Jet Printing, County Supplied Option for discount Pricing c. Automated Inserting on NEW state of the art equipment: Inserting of Absentee voter ballot material per Road Maps (15+ groups) d. Mailware Software: Address accuracy, standardization, and CASS report e. Mail Sort and Preparation	\$0.23 \$0.03 \$0.16 \$0.04 \$0.04
3	Incoming Mail Process- Scheduled Elections and Special Elections <small>Note: (Special Elections are any election outside of the November 5th, 2013 Udel Election, June 3rd, 2014 Primary Election, and the November 4th, 2014 General Election)</small>	a. VoteRemote Signature Capture and Signature Verification scanning process: Signature Capture w/clipped image to VIMS voter registration system b. Flat Fee Scheduled Elections included in Flat Fee <ul style="list-style-type: none"> • November 5th 2013 UDEL • June 3rd, 2014 Primary • November 4th, 2014 General c. Flat Fee Special Elections included in Flat Fee <ul style="list-style-type: none"> • Flat Fee for County Wide Special Elections • Flat Fee for non-County Wide Special Elections *Amount to be invoiced after each election	\$24,400 \$68,518 \$125,582 \$65,000 \$1,000
4	ASR Set-Up	a. One time setup charge per CPU (Each CPU is capable of handling 1.5 million ASR attempts in a 12 month period. During peak years it may be necessary to install a secondary ASR machine.)	\$6,000 (note reduction from \$9,000 in prior contract)
5	Misc. Time & Materials	a. Time & Material charge for non-scheduled processing, maintenance, etc. b. Charge for emergency/rush envelopes c. Other Products or Services as necessary as determined by RR/CC or designee.	\$75.00/HR \$0.08 TBD
6	6% Reduction/Discount	a. Cost reduction/discount (Expires 2/28/15)	6%

DRAFT

August 27, 2013

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, CA 90012

Dear Supervisors:

**RESPONSES TO THE 2012-13 CIVIL GRAND JURY FINAL REPORT
(ALL AFFECTED) (3 VOTES)**

SUBJECT

This letter recommends that the Board: approve the responses to the findings and recommendations of the 2012-13 Civil Grand Jury Final Report; instruct the Executive Officer of the Board of Supervisors to transmit copies of this report to the Civil Grand Jury upon approval by the Board; and instruct the Executive Officer of the Board of Supervisors to file a copy of this report with the Superior Court upon approval by the Board.

IT IS RECOMMENDED THAT THE BOARD:

1. Approve the responses to the findings and recommendations of the 2012-13 Civil Grand that pertain to County government matters under the control of the Board.
2. Instruct the Executive Officer of the Board of Supervisors to transmit copies of this report to the Civil Grand Jury upon approval by the Board.
3. Instruct the Executive Officer of the Board of Supervisors to file a copy of this report with the Superior Court upon approval by the Board.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

Section 933 (b) of the California Penal Code establishes that the county boards of supervisors shall comment on grand jury findings and recommendations which pertain to county government matters under control of those boards.

On June 28, 2013, the 2012-2013 County of Los Angeles Civil Grand Jury released its

Final Report containing findings and recommendations directed to various County and non-County agencies. County department heads have reported back on the Civil Grand Jury recommendations and these responses are attached as the County's official response to the 2012-2013 Civil Grand Jury Final Report.

The recommendations directed to all future Civil Grand Juries have been forwarded to the 2013-2014 Civil Grand Jury for consideration. Recommendations that make reference to non-County agencies have been referred directly by the Civil Grand Jury to those entities.

Implementation of Strategic Plan Goals

The recommendations and responses are consistent with all three of the County Strategic Plan Goals:

- **Goal No. 1 - Operational Effectiveness:**
 - Maximize the effectiveness of the County's processes, structure, and operations to support timely delivery of customer-oriented and efficient public services.
- **Goal No. 2 – Fiscal Sustainability:**
 - Strengthen and enhance the County's capacity to sustain essential County services through proactive and prudent fiscal policies and stewardship.
- **Goal No. 3 – Integrated Services Delivery:**
 - Maximize opportunities to measurably improve client and community outcomes and leverage resources through the continuous integration of health, community, and public safety services.

FISCAL IMPACT/FINANCING

Certain Civil Grand Jury recommendations require additional financing resources. In some cases, financing has been approved by the Board in the current fiscal year's budget. Departments will assess the need for additional funding during the 2013-14 budget cycle, as appropriate.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

In accordance with California Penal Code Section 933 (b), the following departments have submitted responses to the 2012-13 County of Los Angeles Civil Grand Jury Final Report.

ATTACHMENT	DEPARTMENT
A	Chief Executive Office
B	Chief Information Office
C	Children and Family Services
D	County Office of Education
E	District Attorney
F	Executive Office, Board of Supervisors
G	Mental Health (responding for Health Services)
H	Parks and Recreation
I	Probation
J	Sheriff

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Not applicable.

Respectfully submitted,

WILLIAM T FUJIOKA
Chief Executive Officer

WTF:BC:FC
JR:ib

Attachments (10)

c: Sheriff
Executive Office, Board of Supervisors

The Honorable Board of Supervisors
August 27, 2013
Page 4

Auditor-Controller
Chief Information Office
Children and Family Services
County Counsel
County Office of Education
District Attorney
Health Services
Mental Health
Parks and Recreation
Probation

Attachment A

Chief Executive Office



WILLIAM T FUJIOKA
Chief Executive Officer

County of Los Angeles CHIEF EXECUTIVE OFFICE

Kenneth Hahn Hall of Administration
500 West Temple Street, Room 713, Los Angeles, California 90012
(213) 974-1101
<http://ceo.lacounty.gov>

Board of Supervisors
GLORIA MOLINA
First District

MARK RIDLEY-THOMAS
Second District

ZEV YAROSLAVSKY
Third District

DON KNABE
Fourth District

MICHAEL D. ANTONOVICH
Fifth District

July 23, 2013

To: Supervisor Mark Ridley-Thomas, Chairman
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Don Knabe
Supervisor Michael D. Antonovich

From: William T Fujioka
Chief Executive Officer

2012-2013 CIVIL GRAND JURY - FINAL REPORT

Attached are this Office's responses to the 2012-2013 Civil Grand Jury Final Report. We are responding to specific recommendations dealing with the following sections:

- Dual Track and Training – The 2012 Citizen's Commission on Jail Violence Report
- Foster Care Hotline Investigation
- Detention: Adult Facilities

If you have any question regarding our responses, please contact me, or your staff may contact Frank Cheng of this Office at (213) 893-7938, or fcheng@ceo.lacounty.gov.

WTF:BC:FC
JR:ib

Attachment

"To Enrich Lives Through Effective And Caring Service"

**Please Conserve Paper – This Document and Copies are Two-Sided
Intra-County Correspondence Sent Electronically Only**

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – Chief Executive Office, Public Safety Cluster

**SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
Dual Track and Training: 2012 Citizen's Commission on Jail Violence
Report**

RECOMMENDATION NO. 1.2

The Sheriff Department in conjunction with the Board of Supervisors must come to a decision about MCJ. Many of MCJ's issues are unique to this facility. If problems at MCJ have to do with architectural shortcomings, then funding needs to be provided to either rebuild or renovate the facility in accordance with current best practices. Different solutions may be needed for other large scale facilities like Pitchess Ranch or CRDF, as well as Court House Facilities.

RESPONSE

The recommendation has not yet been implemented. The County is currently in the development stages of the capital improvements process for a replacement central jail facility. Any proposed improvements are contingent upon approval by the Board of Supervisors (Board).

Should the Board approve such project improvements and authorize pre-construction studies and design services, the County's project development team will engage justice partners such as the Sheriff's Department, the District Attorney, Alternate Public Defender, Public Defender, and the Department of Mental Health in the programming and design process to ensure operational requirements are addressed.

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – Chief Executive Office, Children and Families Well-Being Cluster

**SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
Foster Care Hotline Investigation**

RECOMMENDATION NO. 4.1

DCFS should initiate in conjunction with the Los Angeles County Board of Supervisors, a separate crisis/information telephone number.

RESPONSE

We are in agreement with this recommendation and will assist DCFS in exploring other Child Welfare jurisdictions to determine their approach to non-child abuse and neglect related calls.

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – Chief Executive Office – Public Safety Cluster

**SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
DETENTION: ADULT FACILITIES**

RECOMMENDATION NO.15.1

The Board of Supervisors and all affected County agencies should vigilantly monitor the additional cost to the detention system caused by AB 109 Realignment.

RESPONSE

This recommendation has been implemented. The Auditor-Controller, CEO, Sheriff, Probation, DMH, DHS, Fire, PD, APD, DA are continuing their collaborative efforts to monitor the additional costs caused by the AB 109.

RECOMMENDATION NO.15.4

The Board of Supervisors should promptly commit to replacing Men's Central Jail as soon as possible with a state of the art facility conforming to best practices in detention.

RESPONSE

The recommendation has not yet been implemented. The County is currently in the development stages of the capital improvements process for a replacement central jail facility. Any proposed improvements are contingent upon approval by the Board of Supervisors (Board).

Should the Board approve such project improvements and authorize pre-construction studies and design services, the County's project development team will engage justice partners such as the Sheriff's Department, the District Attorney, Alternate Public Defender, Public Defender, and the Department of Mental Health in the programming and design process to ensure operational requirements are addressed.

Attachment B

Chief Information Office



RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

Los Angeles World Trade Center
350 South Figueroa Street, Suite 188
Los Angeles, CA 90071

Telephone: (213) 253-5600
Facsimile: (213) 633-4733

July 17, 2013

To: William T Fujioka
Chief Executive Officer

From: Richard Sanchez
Chief Information Officer

2012-13 LOS ANGELES COUNTY CIVIL GRAND JURY FINAL REPORT

In response to your memo dated July 1, 2013, attached is our response to the 2012-2013 Civil Grand Jury Report Recommendation 3.3.

Probation Department Employee Misconduct

Chief Information Office should organize a working group comprised of representatives from the Sheriff's Department, District Attorney, Probation Department, County Counsel and Civil Service Commission in order to establish data entry protocols that produce consistency in all data fields.

If you have any questions regarding this matter, please contact me at 213-253-5600 or rsanchez@cio.lacounty.gov.

RS:pg

Attachment

c: Scott Wiles, Chief Executive Office

P:\Grand Jury\2012-2013 Civil Grand Jury Response.docx

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – CHIEF INFORMATION OFFICE

**SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
PROBATION DEPARTMENT EMPLOYEE MISCONDUCT**

RECOMMENDATION NO. 3.3

Chief Information Office should organize a working group comprised of representatives from the Sheriff's Department, District Attorney, Probation Department, County Counsel and Civil Service Commission in order to establish data entry protocols that produce consistency in all data fields.

RESPONSE

The respondent agrees with the findings.

The recommendation has not yet been implemented, but will be implemented in the future, with a timeframe for implementation.

The Chief Information Office (CIO) has identified and will convene a working group comprised of representatives from departments listed below, as recommended by the Grand Jury, with the goal of establishing data entry protocols that produce consistency in all data fields.

1. Probation Department
2. Sheriff Department
3. District Attorney
4. County Counsel
5. Chief Information Office
6. Civil Service Commission

The initial Work Group meeting to discuss the concerns identified by the Grand Jury and possible solutions will be scheduled this summer. The Working Group will develop an action plan and timetable within 90 days of its first meeting to address data consistency issues.

Attachment C

Children and Family Services



**County of Los Angeles
DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

425 Shatto Place, Los Angeles, California 90020
(213) 351-5602

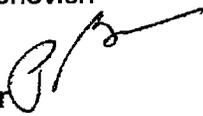
PHILIP L. BROWNING
Director

FESIA A. DAVENPORT
Chief Deputy Director

Board of Supervisors
GLORIA MOLINA
First District
MARK RIDLEY-THOMAS
Second District
ZEV YAROSLAVSKY
Third District
DON KNABE
Fourth District
MICHAEL D. ANTONOVICH
Fifth District

July 19, 2013

To: Supervisor Mark Ridley-Thomas, Chairman
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Don Knabe
Supervisor Michael D. Antonovich

From: Philip L. Browning, Director 

**RESPONSE TO THE 2012-2013 LOS ANGELES COUNTY CIVIL GRAND JURY
RECOMMENDATIONS**

Enclosed please find the Department of Children and Family Services (DCFS) responses to each of the Civil Grand Jury's recommendations for year 2012-2013. The responses to the recommendations have been prepared for the following Civil Grand Jury report section topics: (1) Foster Care Hotline Investigation, (2) Foster Care Quality Assurance Training Foster Parents, and (3) Foster Care Transitional Aged Youth Vocational Training.

If you have any questions, please call me or your staff may call Aldo Marin, Manager, DCFS Board Relations Section, at (213) 351-5530.

PB:HB

c: Executive Officer, Board of Supervisors
Chief Executive Officer
County Counsel

Enclosures

"To Enrich Lives Through Effective and Caring Service"

RECOMMENDATIONS TO THE 2012-2013 GRAND JURY REPORT

APPLICABLE SECTION	LEAD(S)	RECOMMENDATION NUMBER(S)	PAGE NUMBER(S)
Foster Care Hotline Investigation	Children and Family Services (DCFS)	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10	23-33
Foster Care Quality Assurance Training Foster Parents	DCFS	5.1, 5.2, 5.3, 5.4, 5.5	35-41
Foster Care Transitional Aged Youth Vocational Training	DCFS	6.1, 6.2, 6.3, 6.4	43-50

Foster Care Hotline Investigation

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – **DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 4. FOSTER CARE HOTLINE INVESTIGATION

RECOMMENDATION 4.1: DCFS should initiate in conjunction with the Los Angeles County Board of Supervisors, a separate crisis/information telephone number.

RESPONSE: DCFS agrees with the recommendation and will explore other Child Welfare jurisdictions including San Francisco to determine their approach to non-child abuse and neglect related calls. Additionally, DCFS will explore changes that can be made to the existing telephone system to handle and redirect “crisis” calls.

RECOMMENDATION 4.2: DCFS Hotline needs to be reconfigured so that call handlers only take calls from specific regions, for example Pomona, Long Beach, or the San Fernando Valley, in order to be better able to identify local resources.

RESPONSE: DCFS needs further information about this recommendation. While DCFS recognizes the concern made by the Civil Grand Jury, regionalization may not accomplish the stated goal. Technology exists to have calls routed based on area codes or callers could self select based on their zip code but that is not a guarantee that the resources would be better identified. Since 80% or more of the calls are from mandated reporters, most are aware of community resources. Since the majority of the mandated reporters are teachers, followed second by law enforcement, reconfiguration may not achieve the desired outcome. Calls to the Child Protection Hotline by mandated reporters are often related to families who are already involved with community based organizations. However, a Business Plan Re-engineering (BPR) initiative is currently reviewing the Hotline operations and this recommendation will be considered during that process.

RECOMMENDATION 4.3: DCFS must find a method to recognize the specialized performance requirements of the Hotline employee. It must also enhance and reward the work experience for its productive Hotline employees. Most importantly, the Hotline must not be used to accommodate employees who cannot function adequately elsewhere.

RESPONSE: DCFS is in agreement that it is important that all staff assigned to the Child Protection Hotline (CPH) be efficient, effective and capable of handling a large number of calls each day. Additionally, it is recognized that it can be problematic to have staff who not able to perform adequately at the CPH; therefore, CPH managers work in collaboration with the Department’s Human Resources Division to appropriately address personnel and performance issues. The Hotline has a process in place whereby all new staff assigned to the Hotline are interviewed and must have adequate computer skills prior to being accepted. Staff who demonstrate an aptitude for investigative skills are highly desirable. DCFS will explore how best to reward staff assigned at the Hotline, but the goal is that in time all CPH staff are rated as efficient, effective and able to handle a large number of calls.

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – **DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 4. FOSTER CARE HOTLINE INVESTIGATION

RECOMMENDATION 4.4: DCFS must reduce or streamline the policies, procedures and practices that Hotline employees are expected to master.

RESPONSE: DCFS agrees with the recommendation and is in the process of streamlining policies and procedures as part of the Department's Strategic Plan. Hotline staff currently receive an initial 6 to 8 weeks of training on both policy and hands-on training and thereafter continued to be monitored by the training supervisor for an additional 4 to 6 months to ensure the employee has a comprehensive understanding of the expectations and has demonstrated an understanding of the work duties. When new policies, procedures or changes to existing policies are introduced, the Hotline staff receive additional training commensurate with the new or modified policies and procedures.

RECOMMENDATION 4.5: DCFS management must become more directly involved with the actual Hotline calls system by directly experiencing real time calls.

RESPONSE: DCFS partially agrees with the recommendation since senior managers have had an opportunity to observe the Hotline operation, but have not actually handled live calls. All the Hotline managers have taken calls on an as needed basis and are proficient in inputting a report into CWS/CMS. There is a benefit to handling calls directly, but managers are also actively listening and observing the process and steps taken by the staff while multiple calls are handled simultaneously. The Department will encourage all senior managers to visit the Hotline to increase awareness of the volume of calls received and the processes involved in generating and documenting reported calls.

RECOMMENDATION 4.6: DCFS should create a separate phone number from the Hotline for calls involving children who are absent without leave (AWOL) from their foster home or those calls involving "re-placements".

RESPONSE: DCFS agrees with the recommendation and will explore the recommendation of a separate telephone number with the current telephone vendor, as well as, determine what changes can be made to the existing telephone system to accommodate reports that are not critical, but must be documented and require some action on the part of the Department such as AWOLs and request for replacements.

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – **DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 4. FOSTER CARE HOTLINE INVESTIGATION

RECOMMENDATION 4.7: DCFS must reduce the number of unwarranted referrals, by which it is meant those referrals found to be “unfounded”. This can be aided by allowing the Hotline employee to deviate, if need be, from the Structured Decision Making (SDM) tool and rely more on their background and work experience. DCFS needs to allow for regional and cultural differences while ensuring consistency and efficiency.

RESPONSE: DCFS agrees with the recommendation and continues to examine the number of unwarranted referrals to determine if those labeled as “unfounded” truly meet the legal definition for abuse and neglect. Revisions are currently being developed to the SDM tools specific for the Hotline and once completed training will be provided. SDM allows for discretionary input by staff in order to take into account differences as part of the assessment criteria. DCFS management will continue to review and determine if approval is warranted when staff’s assessments include the use of discretionary features to ensure that the rationale for the input is properly documented.

RECOMMENDATION 4.8: DCFS must reduce the scope of the Child Welfare Service/Case Management System (CWS/CMS) applied to urgent Hotline issues. The Hotline should focus on how to respond quickly, gathering only as much information as necessary to make a determination for child abuse or neglect.

RESPONSE: DCFS agrees as the re-design of CWS/CMS at the State level has just started. Los Angeles County has a representative from DCFS assigned to the redesign team. The recommendation will be shared with the representative. Additionally, a recent business process re-engineering involving the Hotline narrative has been recommended and may help to streamline the steps for a quicker completion of the Screener Narrative document in CWS/CMS.

RECOMMENDATION 4.9: DCFS has to aggressively engage the community (e.g. churches, Alcoholic Anonymous, and the like) in its efforts to provide safety for the children in the County. The community’s resources have to be accessed to reduce the need to make “the call”. The Point of Engagement (POE) approach, which shows promise in Torrance, for example, should be deployed countywide.

RESPONSE: DCFS agrees and supports community engagement as part of its efforts to keep children safe. Families are encouraged to use community resources and only make “the call” when there is no other recourse. Currently regional offices are holding meetings with community partners and the Department continues to examine how to expand this effort, thereby decreasing the negative myths and stereotypes that exist in the community about DCFS.

“To Enrich Lives Through Effective and Caring Service”

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – **DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 4. FOSTER CARE HOTLINE INVESTIGATION

RECOMMENDATION 4.10: DCFS should expand the pool of employees who are available to work at the Hotline to include those applicants without social work backgrounds. It must recognize the specialized nature of Hotline work and include persons with, for example, police backgrounds, in its applicant pool. This recommendation is similar to that made in 2012 by the CSIU.

RESPONSE: DCFS partially agrees as all employees at the Hotline must meet the same qualifications as all other Children's Social Workers (CSW) who work for the Department. Currently, the minimum educational qualification for a Children's Social Worker Trainee is a bachelor's degree in psychology, sociology, social work, child development, or a related human services field. DCFS would not exclude individuals with law enforcement backgrounds as long as they meet the basic required qualifications. DCFS does not actively recruit applicants with law enforcement or investigative backgrounds, but instead recruits candidates based on the required and desirable qualifications aforementioned. If DCFS were to move forward with this recommendation it would need to work closely with the County's Human Resources Division to determine how best to incorporate this group of applicants into the desired positions.

Foster Care Quality Assurance Training Foster Parents

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – DEPARTMENT OF CHILDREN AND FAMILY SERVICES

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 5. FOSTER CARE QUALITY ASSURANCE TRAINING FOSTER PARENTS

RECOMMENDATION 5.1: DCFS must assess, upgrade, and standardize the scope and sequence of the foster parent training curriculum emphasizing evidence-based practices

RESPONSE: The Department agrees with the recommendation that trainings should encompass the topics of Post-Traumatic Stress Disorder (PTSD), coping behaviors, critical thinking and conflict management. Training skills practice must emphasize values, communication, behavior management, financial literacy, time management, peer pressure, nutrition and exercise to best prepare foster parents.

The Adoption and Permanency Resources Division of DCFS, Resource Family Assessment Units have a workgroup that has been reviewing the PS-MAPP curriculum for updates to provide the most up-to-date information and evidence-based concepts to prospective caregivers. Currently, the curriculum addresses the behaviors of PTSD in meeting 2, coping behaviors in meeting 3, all of meeting 5 is devoted to behavior management, critical thinking in meetings 2 through graduation, and conflict management is embedded in each meeting. Meetings 2 through graduation also have a skills practice with group interaction component, with values, communication, and behavior management woven into the curriculum. Practice for skills with peer pressure, time management, nutrition and exercise are included in meeting 7 and meeting 9. The PS-MAPP curriculum workgroup will examine ways to incorporate financial literacy into the six week program.

The PS-MAPP curriculum will be enhanced during the next year using the National Child Traumatic Stress Network's (NCTSN) Caring for Children Who Have Experienced Trauma curriculum. The NCTSN has collaborated closely with the National Crime Victims Research and Treatment Center at the Medical University of South Carolina. This curriculum has also been offered as continuing education for foster caregivers through the Foster Care Kinship Education program funded by the California Community College Chancellor's Office.

Additionally, the Kit for New Parents offered by First 5 California is now being given to all PS-MAPP participants after Meeting 3. The kit contains parenting advice and tips on nutrition, safety, discipline, early learning, and quality child care. A study published in the American Journal of Public Health in 2007 found that mothers who used the English or Spanish Kit demonstrated improved parenting skills.

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – DEPARTMENT OF CHILDREN AND FAMILY SERVICES

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 5. FOSTER CARE QUALITY ASSURANCE TRAINING FOSTER PARENTS

RECOMMENDATION 5.2: DCFS must train foster parents and a cadre of master teachers within the proposed DCFS Inter-University Consortium Training Academy.

RESPONSE: Licensed foster parents in Los Angeles County are required to complete annual renewal training hours to maintain their licenses. This training is available through the 14 local Community Colleges who offer a variety of renewal training classes for licensed foster parents. Additionally, the DCFS Training Section coordinates and provides an array of specialized in-service and large scale quality training events that are open to not only licensed foster parents but also open to related and non-related caregivers, adoptive parents and legal guardians. All Training Opportunities are aimed at promoting and achieving Departmental priorities of child safety, timely/legal permanency, and to reduce the reliance of out- of-home care.

The training section is currently working together with the PS-MAPP DCFS program manager on a contract that will allow direct contracting with the Community Colleges to deliver trainings on an as needed and on as requested basis. Please find below a partial list of the trainings, conferences and seminars offered over the past several years.

Annual Conferences:

Mi Casa Es Su Casa Training Conference	Annual Fatherhood Solutions Conference
National Foster Parent Association Education Conference	Latino Behavioral Health Conference

In-Service/Specialized Trainings have included the following:

Abuse and children with Development Disabilities	Obesity: The Physical Effects Obesity: Treatment
Cyber bullying & Sexting: What Caregivers Need to Know	Whole Family Foster Home
Healthy Child & Adolescent Sexuality	Anger Management
Signs and Symptoms of Diabetes	Respiratory Potpourri
Asthma Basics	Perinatal Drug and Alcohol Exposure
Strengthening Access to Dental Services for Children under DCFS Care	Teen Suicide
Multidisciplinary Assessment Team	Oppositional Defiant Disorder/Disruptive Behavior Disorder
Learning Disabilities	The Impact of Trauma on Children, Youth and Families
Helping Resource Families Navigate through the Educational System	Whooping Cough
Individualized Education Plans	Allergies
Suspensions, Truancies, and Absences	Impact Of Trauma On Neuro-Development In Early Childhood
Visitations	Guide to Learning Disabilities
Child & Adolescent Sexual Development	Prenatal Alcohol Exposure & Fetal Alcohol Spectrum Disorder
Sensory Processing	Understanding ADHD
Impulse Control	Failure to Thrive

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – **DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 5. FOSTER CARE QUALITY ASSURANCE TRAINING FOSTER PARENTS

RECOMMENDATION 5.3: DCFS must quickly implement the Strategic Plan training objectives for foster parents.

RESPONSE: DCFS agrees since the Strategic Plan Objective 1.2.2 requires that the Department recruit an additional 10% of qualified, committed and dedicated foster homes in proportion to the needs of each community; and provide these caregivers with training designed to promote child safety and address the needs of abused and neglected children.

The DCFS Strategic Plan Objective Team (SPOT) workgroup focusing on this objective is comprised of nine staff members representing eight different Regional Offices and Divisions. The workgroup has met monthly to address the recruitment of new Resource Parents who desire to provide foster care. As of July 15, 2013, 34 families who expressed interest in becoming foster parents have been approved and are eligible to take out of home placements. The National Resource Center for Diligent Recruitment at AdoptUSKids has been asked to provide technical assistance to Los Angeles County and is assisting the workgroup in examining recruitment and training strategies for new Resource Parents. As noted for Recommendation 5.1, there is a PS-MAPP curriculum workgroup, which will examine ways to reinvigorate the six week program curriculum.

As noted in Recommendation 5.1, the PS-MAPP curriculum will be enhanced during the next year using the National Child Traumatic Stress Network's (NCTSN) Caring for Children Who Have Experienced Trauma curriculum. The NCTSN has collaborated closely with the National Crime Victims Research and Treatment Center at the Medical University of South Carolina. This curriculum has also been offered as continuing education for foster caregivers through the Foster Care Kinship Education program funded by the California Community College Chancellor's Office.

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – **DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 5. FOSTER CARE QUALITY ASSURANCE TRAINING FOSTER PARENTS

RECOMMENDATION 5.4: DCFS must assign greater value to foster parent input within its multidisciplinary teams.

RESPONSE: DCFS agrees with the recommendation. Foster parents are currently included when a Multidisciplinary Assessment Team (MAT) assessment is conducted -- they are asked to participate during both the assessment process and at the summary of findings meeting. In addition, Child and Family Teams (CFT) are being piloted in four offices (Pomona, Compton, Wateridge and Torrance) with a tentative plan to implement in up to four additional offices by November. CFT members include everyone who is important to the child and family, including caregivers. The intent of the CFT is to function on an ongoing basis to develop the most appropriate plans and supports for the child and family. The caregivers are in a unique position as they know the child very well and their input is crucial in the development of an appropriate case plan.

RECOMMENDATION 5.5: DCFS must restructure its electronic data network to transmit client information on demand to all involved caregivers.

RESPONSE: DCFS agrees with the recommendation. On July 15, 2013, BIS implemented the Foster Care Search System - Caregiver Home Profile website through the DCFS Internet site. This website portal will allow licensed foster parents to access and input their basic information, including listing the number of foster children residing in the home, and the specific population they are licensed to serve in order to begin to provide DCFS staff on demand and up to date information of available foster homes.

Foster Care Transitional Aged Youth Vocational Training

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – **DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 6. FOSTER CARE TRANSITIONAL AGED

RECOMMENDATION 6.1: DCFS should assess all foster care youth under its jurisdiction, 16-24 years old who do not have a high school diploma to determine whether a dual track approach is beneficial. This would combine academic and vocational training in order to enhance opportunities for employment

RESPONSE: DCFS partially agrees with this recommendation. With the January 1, 2012 implementation of Assembly Bill 12 (AB12), the length of the DCFS' jurisdiction over foster youth extends up to the age of twenty-one. DCFS agrees to assess all foster youth under its jurisdiction between the ages of 16 years through 21, who do not possess a high school diploma to determine whether a dual track approach would be beneficial. DCFS jurisdiction does not extend to youth beyond the age of 21.

The recommendation has not been implemented by DCFS. By December 31, 2013, DCFS Training Section will develop curriculum and begin training in the utilization of case planning strategies developed in partnership with caregivers and youth that focus on enhancing the emancipation skills of adolescents and young adults. A specific focus of the training will be to ensure that all youth aging out of the public child welfare system without a high school diploma are on track to benefit from exposure to a vocational approach and existing opportunities, including YouthBuild (6.2) and the Los Angeles Unified School District's (LAUSD) Alternative Education and Work Center Program (AEWC).

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – **DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 6. FOSTER CARE TRANSITIONAL AGED

RECOMMENDATION 6.2: DCFS should assign a coordinator to begin a pilot program to encourage a significant number of foster youth to participate in the YouthBuild Charter School of California (YouthBuild) or similar program.

RESPONSE: DCFS agrees with this recommendation. The recommendation was implemented by DCFS on May 29, 2013, one Children Services Administrator II has already been designated the DCFS coordinator for a pilot program designed to foster increased youth participation in YouthBuild Charter School of California, as well as, to promote collaborative work between DCFS and YouthBuild Charter School of California. The project strategies include the development of a YouthBuild Resource informational fact sheet, including site locations, to be posted on DCFS' intranet (LAKIDs), as well as, active through the active promotion and outreach of this alternate educational/vocational opportunity at general staff meetings, supervisory meetings and by DCFS' contracted Education Consultants.

RECOMMENDATION 6.3: DCFS should strive to enroll more students in the Los Angeles Unified School District's (LAUSD) Alternative Education and Work Center Program (AEWC). The foster parent, guardian or DCFS case worker should work directly with the AEWC consultant at each location to enroll youth in the AEWC program

RESPONSE: DCFS agrees with this recommendation. This recommendation has not been implemented. By December 31, 2013, DCFS will begin providing training for all social work staff on alternate vocational program opportunities for foster youth who have yet to graduate from high school. By educating DCFS social work staff on programs such as AEWC, foster youth enrollment into these programs should increase. In the interim, by November 1, 2013, DCFS will issue a For Your Information (FYI) staff informational notice that will inform all social work staff of alternate vocational program opportunities for their transition age foster youth and how to access these opportunities for eligible youth.

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – **DEPARTMENT OF CHILDREN AND FAMILY SERVICES**

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 6. FOSTER CARE TRANSITIONAL AGED

RECOMMENDATION 6.4: DCFS should begin training classes for case workers, group home supervisors, counselors and especially the foster parents to assure that all youth aging out without a high school diploma are on track to benefit from exposure to a vocational approach.

RESPONSE: DCFS agrees with this recommendation. This recommendation has not been implemented by DCFS. In addition to departmental training plans detailed in the response for Recommendation 6.1, the DCFS Training Section will concurrently develop and implement a training module by March 1, 2014. The proposed training will be equivalent to the “Train the Trainer” module and will be provided to all contracted Foster Family Agencies (FFAs) and Group Homes so they can in turn train their certified parents and staff.

Attachment D

County Office of Education



Los Angeles County Office of Education

Leading Educators ▪ Supporting Students ▪ Serving Communities

Arturo Delgado, Ed.D.
Superintendent

July 18, 2013

Los Angeles County
Board of Education

Rebecca J. Turrentine
President

Katie Braude
Vice President

Douglas R. Boyd

José Z. Calderón

Rudell S. Freer

Thomas A. Saenz

To: Supervisor Mark Ridley-Thomas, Chairman
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Don Knabe
Supervisor Michael D. Antonovich

From: Arturo Delgado, Ed.D.
Superintendent

A handwritten signature in black ink that reads "Arturo Delgado".

Subject: RESPONSE TO THE 2012-2013 LOS ANGELES COUNTY
CIVIL GRAND JURY FINAL REPORT

In accordance with the request from the Los Angeles County Chief Executive Officer dated July 1, 2013, attached is the Los Angeles County Office of Education (LACOE) response to the Civil Grand Jury recommendation that pertains to LACOE operations.

AD/CA/PW:sb
Attachment

cc: Sachi A. Hamai, Executive Officer, Board of Supervisors
William T Fujioka, Chief Executive Officer
John Krattli, County Counsel
Jerry Ramirez, Quality and Enrichment Program Services
David Sommers, Public Information Officer

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – LOS ANGELES COUNTY OFFICE OF EDUCATION

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
DETENTION: JUVENILE FACILITIES

RECOMMENDATION NO. 16.6.

The Department of Probation and the Los Angeles County Office of Education should implement innovative reading programs to increase the reading decoding and comprehension levels of juveniles at all of the Camps.

RESPONSE

The Probation Department and the Los Angeles County Office of Education agree with this recommendation. The recommendation has been implemented and will continue to undergo improvements in implementation to maximize student performance outcomes. Below outlines innovative reading programs currently offered at Juvenile Camp Schools to increase reading decoding and comprehension levels. Each program offers a rich source of data instrumental to program monitoring and student-centered decision-making at each school site.

Achieve3000

Achieve3000 is a reading intervention program designed to improve student reading through core instruction in both state content standards and common core standards. Ongoing assessments are built into the daily instructional routine, which provide performance data to guide the decision-making process and facilitate progress monitoring.

Scholastic READ 180

READ 180 is a program designed for students whose reading achievement is two or more years below grade level. It is a reading intervention program that provides scientifically based, explicit, and systematic instruction that addresses individual needs through adaptive instructional software, high-interest literature, and direct instruction in reading and writing. The instructional model is set in three rotations: whole group direct instruction, small group instruction, and individualized computer instruction. Students receive constant feedback on their progress in both the computer work and teacher-led lessons. Students are formally reassessed every 60 days to monitor reading lexile growth and ensure proper progress in the program.

Scholastic System 44

System 44 is a component of the READ180 program and is designed for the most challenged older readers, whose achievements in reading range from non-reader through grade four. The program addresses the foundational elements of the English language, providing a strong base in phonemic awareness, phonics, decoding, morphology, and orthography, in a manner that is palatable to the older student. Students work through levels of instruction until all decoding gaps are filled and then move into the READ 180 program to further their instruction in academic vocabulary, comprehension, and writing.

2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
DETENTION: JUVENILE FACILITIES

Page 2

After-School Extended Learning Opportunities (ELO) Program

Students may extend their learning beyond the school day in the after-school ELO Program. This program includes a small student-to-teacher ratio. Students are offered CAHSEE Prep, GED Prep, and Language Arts intervention curriculum. Reading support is imbedded in the ELO curriculum to ensure student success.

Freedom Schools

Freedom Schools is a five-week reading enrichment program sponsored by the Children's Defense Fund. The program is designed to engage students in reading through a research-based and multicultural curriculum that supports children and families around five essential components: high quality academic enrichment; parent and family involvement; civic engagement and social action; intergenerational leadership development; and nutrition, health, and mental health. Freedom Schools is being piloted during the summer of 2013 at two LACOE schools, Afflerbaugh and Miller.

Operation Read

Operation Read is a Probation-operated tutoring program designed to build students' literacy skills in reading, comprehension, writing, and spelling. Academic mentors work with students one-to-one and in small groups, three to five hours per week, to provide a variety of instructional approaches that are individualized to each student.

During the 2012-13 school year, each intervention program went through a thorough study involving data analysis to determine the level of implementation and effectiveness of each program. A committee reviewed the findings, interpreted the data, and generated recommendations to improve program implementation and effectiveness. In efforts to ensure ongoing teaching and learning and, therefore, reading outcomes, a follow-up study for each reading intervention program will be conducted in the coming months to maintain program quality and integrity. In the interim, site leadership teams will continue to analyze reading achievement data within their Professional Learning Communities (PLCs). This PLC analysis informs teachers on student learning and allows them to develop innovative strategies to improve students' decoding and comprehension levels on a weekly basis.

Attachment E

District Attorney



JACKIE LACEY
LOS ANGELES COUNTY DISTRICT ATTORNEY

18000 CLARA SHORTRIDGE FOLTZ CRIMINAL JUSTICE CENTER
210 WEST TEMPLE STREET LOS ANGELES, CA 90012-3210 (213) 974-3501

July 19, 2013

TO: Supervisor Mark Ridley-Thomas, Chair
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: Jackie Lacey 
District Attorney

SUBJECT: **RESPONSE TO THE 2012-2013 LOS ANGELES COUNTY CIVIL
GRAND JURY FINAL REPORT**

Attached is my Department's response to the recommendation contained in the following section of the 2012-2013 Los Angeles County Civil Grand Jury Final Report:

Detention Adult Facilities

Your staff may contact Lynn Vodden, Director of the Bureau of Administrative Services at (213) 202-7616, if they have any questions or require additional information.

lv

Attachment

c: William T Fujioka
Chief Executive Officer

RESPONSE TO THE GRAND JURY FINAL REPORT
COUNTY OF LOS ANGELES – DISTRICT ATTORNEYS OFFICE

**SUBJECT: 2013-2014 CIVIL GRAND JURY RECOMMENDATION FOR
DETENTION ADULT FACILITIES**

RECOMMENDATION NO. 15.2:

The Los Angeles County District Attorney should continue to identify and encourage alternatives to incarceration for low level offenders.

RESPONSE

We concur with the Civil Grand Jury's recommendations that the Los Angeles County District Attorney should continue to identify and encourage alternatives to incarceration for low level offenders, in a manner which is consistent with public safety.

The Los Angeles County District Attorney's Office currently sponsors six different alternative sentencing programs: Drug Court; Sentenced Offender Drug Court (SODC); Veterans Court; Second Chance Women's Re-Entry Court; Co-Occurring Disorders Court, and Homeless Court. The District Attorney's Office continues to actively assess the effectiveness of each program and consider possible expansion of the existing programs as well as the possible creation of new programs.

In addition, this Office continues to actively discuss alternative sentencing with other County departments, through the Countywide Criminal Justice Coordination Committee (CCJCC), including the Los Angeles County Sheriff's Department. This Office is committed to fully considering and implementing appropriate alternatives to jail incarceration.

Attachment F

Executive Office, Board of Supervisors



SACHI A. HAMAI
EXECUTIVE OFFICER

COUNTY OF LOS ANGELES BOARD OF SUPERVISORS

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 383
LOS ANGELES, CALIFORNIA 90012
(213) 974-1411 • FAX (213) 620-0636

MEMBERS OF THE BOARD

GLORIA MOLINA
MARK RIDLEY-THOMAS
ZEV YAROSLAVSKY
DON KNABE
MICHAEL D. ANTONOVICH

July 19, 2013

TO: William T Fujioka
Chief Executive Officer

FROM: Sachi A. Hamai 
Executive Officer

SUBJECT: RESPONSES TO THE 2012-13 LOS ANGELES COUNTY CIVIL GRAND JURY
FINAL REPORT

This is to provide you with our response to the recommendations made by the Los Angeles County Civil Grand Jury in their 2012-13 final report.

We are in agreement with the recommendations proposed in Section 7: Board of Supervisors – Request and Complaint Procedures. Please find attached our response to these items.

If you have any further questions, please contact Patrick Ogawa of my staff at (213) 974-1403. Thank you.

SAH:po:sg

Attachment

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – BOARD OF SUPERVISORS

**SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
SECTION 7 – REQUEST AND COMPLAINT PROCEDURES**

RECOMMENDATION NO. 7.1

The offices of the Supervisors of the Second, Third, Fourth, and Fifth Districts of the Los Angeles County Board of Supervisors should modify their “web contact forms” to repeat the entire contents when submitted (see Finding 5). This is done on the “web contact form” of the First District. Currently, the other districts just acknowledge submission, but the First District provides a printable copy of everything entered into the form. This allows the Constituent to verify and save a copy of the request.

RESPONSE

The Executive Office is working with each of the Board offices to establish a web contact form that is flexible and workable for each of their offices.

RECOMMENDATION NO. 7.2

The offices of each of the Supervisors should continue to ensure that their staff has up to date computers so the staff can adequately use the Constituent Relationship Management system (CRM).

RESPONSE

The Executive Office Information Resource Management (IRM) has an ongoing 3-year PC refresh cycle that has been in place for over 7 years. IRM continues to work with all Board offices to refresh their PCs as necessary due to the performance demand using the CRM application and web services by each Board office. From time to time, IRM will receive requests to replace PCs that are underperforming due to hardware and/or software issues. IRM has mitigated those requests usually within the same day or within a couple of days by either replacing the PC or parts under warranty, reloading software packages, or reinstalling windows operating systems, etc. All computers in the Board of Supervisors offices have been reviewed and inspected to confirm that they all have up to date systems. This office will continue to make sure all Board staff are equipped with high functioning computers that allow them to adequately use the CRM system.

RECOMMENDATION NO. 7.3

The offices of all the Supervisors should have staff representatives meet twice a year to share information on resources available for answering constituent requests. The districts would benefit from sharing process and procedures, and discussing use of CRM.

RESPONSE

Board offices will communicate and share information and resources between their respective offices. They will share ideas amongst themselves on how to promote and improve overall customer service for their constituencies. The Executive Office will continue to share updates on the CRM, so that Board staff can maximize their utilization of this system.

RECOMMENDATION NO. 7.4

The office of the Fourth Supervisorial District should enter all requests requiring follow-up into the CRM system. Logging requests should not be restricted to those submitted through letters; but include requests through email, web contact form, fax, personal contact, and phone.

RESPONSE

The Executive Office will continue to work in maximizing the usage of the CRM system. IRM staff has provided training and technical assistance for all district staff and will continue to assist Board offices on all hardware and software needs.

Attachment G

Mental Health



LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH
550 S. VERMONT AVE., LOS ANGELES, CA 90020 HTTP://DMH.LACOUNTY.GOV



MARVIN J. SOUTHARD, D.S.W.
Director
ROBIN KAY, Ph.D.
Chief Deputy Director
RODERICK SHANER, M.D.
Medical Director

July 24, 2013

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
Los Angeles, California 90012

Dear Members of the Civil Grand Jury:

**RESPONSE TO THE FINAL REPORT OF THE
2012-13 LOS ANGELES COUNTY CIVIL GRAND JURY**

Attached is the Los Angeles County Department of Mental Health's response to the 2012-13 Civil Grand Jury Report recommendations. The Civil Grand Jury's area of the Dual Track and Training 2012 Citizen's Commission on Jail Violence Report, Recommendation 1.6.

Should you have questions regarding our response, please contact me, or your staff can contact Dr. Stephen Shea at (213) 974-9083.

Sincerely,

Marvin J. Southard, D.S.W.
Director

MJS:tb:mb

Attachment

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES — DEPARTMENT OF MENTAL HEALTH

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
DUAL TRACK AND TRAINING

RECOMMENDATION No. 1.6

The Sheriff's Department in conjunction with the Department of Health needs to significantly increase mental health training Department-wide. The Department needs to work with other entities (Department of Mental Health, the county's e-education system, non-profits and private enterprise) to come up with ways to disseminate this training without causing positions to be backfilled while officers attend the training. Specifically, more needs to be taught relating to Post Traumatic Stress Disorder (PTSD), trauma and the behaviors that may result as well as de-escalation techniques.

RESPONSE

The Department agrees with this recommendation. Department of Mental Health (DMH) in coordination with the Sheriff's Custody Training Bureau currently provides mental health training to all newly assigned custody personnel. In addition, the Custody Training Bureau partnered with DMH to create a shared internet link that can be accessed by Sheriff's staff. The link has a series of videos that addresses basic mental health issues, mental health scenarios and information on how to deal with the mentally-ill population. Mental Health staff at the jail also provides training in Suicide Prevention, Jail Operations and Introduction to Mental Health and Custody Triage. Along with the Sheriff's Department, DMH will work to implement training in Post-Traumatic Stress Disorder (PTSD), trauma and de-escalation techniques.

Attachment H

Parks and Recreation



COUNTY OF LOS ANGELES
DEPARTMENT OF PARKS AND RECREATION

"Parks Make Life Better!"

Russ Guiney, Director

John Wicker, Chief Deputy Director

July 19, 2013

TO: William T. Fujioka
Chief Executive Officer

FROM: Russ Guiney *by Robert Maycumber*
Director

SUBJECT: **RESPONSES TO THE 2012-13 LOS ANGELES COUNTY CIVIL GRAND
JURY REPORT**

As requested, the Department of Parks and Recreation has reviewed the final 2012-13 Civil Grand Jury Report. Attached is the completed response document.

If your staff requires any additional information, please have them contact Monica Pollaccia of Management Services at (213) 738-3226.

RG:JW:RAM:MR:EM:mp

Attachment

RESPONSE TO THE GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – PARKS AND RECREATION

SUBJECT: 2012-2013 GRAND JURY RECOMMENDATIONS FOR
PARKS and RECREATION

RECOMMENDATION NO 9.1

County of Los Angeles Department of Parks and Recreation (Department) and the City of Los Angeles Department of Recreation and Parks should provide an operations manual to all park managers.

RESPONSE

The Department agrees with the finding. The Department plans on implementing this recommendation and will ensure that operation manuals are developed for all park managers in every Agency by July 1, 2014.

The Department Head sent out a memo on July 19, 2013, to *All Parks and Recreation Staff* making them aware of the recommendation and to ensure that corrective actions are followed.

RECOMMENDATION NO 9.2

County of Los Angeles Department of Parks and Recreation should display the United States flag at Bethune Park, DeLongpre Park and Ted Watkins Park.

RESPONSE

The Department agrees with the finding and has displayed the United States flag at Bethune Park and Ted Watkins Park, effective July 11, 2013. DeLongpre Park is not a Department Park. The facility is operated by the City of Los Angeles Department of Recreation and Parks.

RECOMMENDATION NO 9.3

County of Los Angeles Department of Parks and Recreation should provide greater security at Kenneth Hahn State Recreation Area.

RESPONSE

The Department agrees with the finding and has taken measures to improve the security at Kenneth Hahn State Recreation Area. The Department installed 11 security light poles from the kiosk extending up the road to the main office on May 13, 2013. In addition, the Department plans on installing a video security surveillance system at the entrance kiosk by December 15, 2013.

Attachment I

Probation



**COUNTY OF LOS ANGELES
PROBATION DEPARTMENT**

9150 EAST IMPERIAL HIGHWAY – DOWNEY, CALIFORNIA 90242
(562) 940-2501



JERRY E. POWERS
Chief Probation Officer

July 19, 2013

TO: Supervisor Mark Ridley-Thomas, Chairman
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: Jerry E. Powers *JEP for J.P.*
Chief Probation Officer

SUBJECT: RESPONSE TO THE 2012-2013 GRAND JURY'S FINAL REPORT

Enclosed is the Probation Department's response to the Civil Grand Jury's recommendations contained in their 2012-2013 Final Report.

If you have any questions or need additional information, please contact Don Meyer, Assistant Chief Probation Officer at (562) 940-2851.

JEP:FC:ld:za

Enclosures

c: William T Fujioka, Chief Executive Officer
Jerry Ramirez, Chief Executive Office



COUNTY OF LOS ANGELES PROBATION DEPARTMENT

9150 EAST IMPERIAL HIGHWAY – DOWNEY, CALIFORNIA 90242
(562) 940-2501



JERRY E. POWERS
Chief Probation Officer

July 19, 2013

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – PROBATION

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
PROBATION DEPARTMENT EMPLOYEE MISCONDUCT

RECOMMENDATION NO. 3.1

The Probation Department should continue to hire new employees who only fall into Bands 1 and 2 of the applicant pool and increase recruiting at local colleges and universities.

RESPONSE

Probation generally agrees with this recommendation; however, we believe that with the new safeguards that have been implemented in the background process we can hire candidates in band 3 and still ensure that the candidates meet our high expectations. In order to understand how this problem came to be, some historical context must be provided.

PAST HIRING PRACTICES

Within the past several years it has become clear to Probation Department management that past hiring practices and standards have resulted in the hiring of some employees who did not meet the high standards and expectations commensurate with a law enforcement agency. Several high profile arrests as well as an unacceptably high level of internal misconduct allegations have troubled the Department for the past several years.

CURRENT BACKGROUND PROCESS

As a result of AB 109 (Realignment), the Department has recently embarked upon a new campaign to bring in a large number of staff in a short amount of time. Reminiscent of aforementioned problems that occurred with the last "mass hiring," there is a great deal of external pressure on the Department to rapidly fill vacant positions. AB 109 clientele have been released from State custody and are now under the supervision of the Probation Department. Unlike the previous hiring campaign, the department has implemented a comprehensive and rigorous background process to include the following:

Rebuild Lives and Provide for Healthier and Safer Communities

- More comprehensive personal history review to include credit history checks and social media review
- Field reviews on potential candidates, where Probation staff canvass a candidate's neighborhood to gather information from neighbors
- Polygraph exams – Probation has contracted with the Los Angeles County Sheriff's Department to provide polygraph services for potential candidates
- Better collaboration with our contract Psychiatrist to ensure that all information including polygraph results, is presented to and considered

This more stringent process has resulted in a delay in filling critical vacancies. Hundreds of candidates have been processed and placed into bands 1, 2 and 3; however, less than 50 candidates have made it into the 2 academy classes held this year. Of those, several candidates have dropped out of the academy for various reasons.

RECRUITMENT

Over the past decade Probation's recruitment efforts have been sporadic and inconsistent. There have been outreach efforts in the past whereby Probation staff have manned booths at various hiring events. However, the majority of candidates for recent exams appear to be "word of mouth" referrals and an unusually high number of candidates appear to have relatives or friends within the Department. Also, during periods where other law enforcement agencies are hiring, Probation has had to compete for candidates with other agencies such as Los Angeles Police Department (LAPD) and the Los Angeles Sheriff's Department (LASD); agencies that have very robust recruitment and outreach efforts. Probation has historically dedicated very little in the way of resources to market the Department. Additionally, the Department has limited college outreach to community colleges; due in part to the fact that entry level positions require either a high school diploma or 60 units of college. Four year universities were not consistently targeted for outreach.

In the past several months the Department has embarked upon a multi-faceted approach to address the recruitment issue. The Department's Media Consultant has spearheaded a campaign to create a more robust message delivery system, which will include a multi-media approach. In July 2013, Probation management and Human Resources staff met with the Los Angeles County Fire Department Training Division to learn about their Turnout and Blackboard web campaigns. Probation is considering contracting with a video production company to create video vignettes, featuring a variety of staff from different functions in an effort to educate the public about Probation and the varied assignments that make up the Department.

Additionally, the Department has begun to reach out to local universities and will attempt to recruit not only traditional candidates with a criminal justice background, but candidates who have backgrounds in sociology or other related interests. By expanding outreach and seeking a broader candidate base, it is anticipated that the quality of candidates will increase dramatically and give Probation the ability to choose the "best of the best".

RECOMMENDATION NO. 3.2

The Probation Department should use its best efforts to retain experienced supervisory staff at its juvenile halls and camps while otherwise meeting the staffing needs mandated by AB 109 Realignment.

RESPONSE

On January 10, 2006, the authorized Management Representative of the County of Los Angeles (hereinafter “County”) and American Federation of State, County and Municipal Employees Local 685 (AFSME or “Union”) approved and ordered implemented by the County’s Board of Supervisor enacts necessary amendments to all County ordinances, including the Los Angeles County Code required to implement the full provisions of articles. Article 16 – Reassignments and Promotions/Probation sets forth reassignment procedure.

Section G of the Article states:

Employees seeking reassignments to other work locations will, providing that the last three Performance Evaluation of record is at least competent and provided that the employee has a minimum of two years in the current work location, submit to the Personnel Services Office (Human Resources (HR) Division) a bid or bids by the last working day of any given month.

As a result of this agreement between County and the Union, the retention of the most highly skilled peace officers in the Department’s juvenile halls and camps is difficult to achieve and maintain.

Also, it should be noted that the Executive Summary, No. 2 of the Grand Jury Report (page 19) states in pertinent part: “Further, a balance must be struck so that the experienced probation officers in the camps are not the sole of hire into these positions.” To that end, the Probation Department has been able to recruit and select candidates from the open list that are hired directly from the community and placed into probation officer positions in the community. As an example, on the most recent DPO II list, five (5) staff was hired into the positions from the community.

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
DETENTION: JUVENILE FACILITIES

RECOMMENDATION NO. 16.1

The Department of Probation should expand the Advanced Path Academy credit recovery program to all Camps.

RESPONSE

The Probation Department agrees with this recommendation. The Advanced Path Academy uses software provided by Apex Learning in their academies. The Los Angeles County Office of Education (LACOE) has licensed the credit recovery software directly from Apex Learning. By doing this, LACOE is able to provide the same rigorous standards-based credit recovery program offered in the Advanced Path Academy, at a significant cost savings. The Probation Department is supporting LACOE's rollout of the Apex Learning Labs at all of the Probation camps and Halls. The plan is to have these labs in operation at all of the Los Angeles County Probation Camps and Halls by early 2014.

RECOMMENDATION NO. 16.2.

The Department of Probation should provide vocational/occupational training programs at all Juvenile Camps without further delay.

RESPONSE

The Probation Department agrees with this recommendation. Vocational/ occupational training programs are currently offered at eleven of the fourteen Juvenile Camps. Both the Probation Department and LACOE will work collaboratively during the 2013-2014 school year to offer vocational/occupational training programs at the three remaining camps. In addition, both agencies plan to expand the vocational/occupational training programs that are currently in operation.

RECOMMENDATION NO. 16.3.

The Department of Probation should rigorously monitor the assignment of juveniles to lessen and prevent youth-on-youth violence by eliminating multiple members of the same gang or competing gangs being assigned to the same Camp.

RESPONSE

The Probation Department agrees with this recommendation. Approximately 2,400 youth receive camp placement orders annually. A large proportion of these youth have gang affiliations. When a youth is ordered to camp, the Probation Department provides a

comprehensive assessment to determine the most appropriate housing location for that youth. A number of factors determine the camp selection, including, but not limited to:

- The gender of the youth
- The medical needs of the youth
- The mental health needs of the youth
- The educational needs of the youth
- Programming needs including the Youth Opportunity Block Grant (YOBG)
- Security concerns (Codes)
- Court ordered or identified keep-away youth, including victims
- Age
- Treatment needs
- Family reunification concerns
- Court recommendations

The first four criteria are concrete in nature and are not open to interpretation. The medical needs of the youth override other housing considerations, including gang affiliation. However, the youths' gang ties and associations are still considered in reviewing criminal partnerships, and are factored into the decision making process.

The camps utilize the Multi-Disciplinary Team (MDT) approach to identify the elements impacting each youth's behavior and needs. This is the forum to address gang issues and interventions tailored to the individual youth, and in relation to the camp community as a whole. The staff at every camp identifies their gang members, and has an understanding of the gang dynamics at their camp. If they conclude that the intake of a specific gang should be curtailed, the Probation Department will move to accommodate that request. The Probation Department also holds a monthly meeting to discuss matters of intake concern with the camps and probation partners. Gang concerns are an ongoing item of discussion. Information that assists the camps in adjusting to the issues of gang conflict in camps and the community is shared. However, it is not possible to limit gang representation to single youth in any one camp, nor is it appropriate to segregate based on gang affiliation. Such segregation by gangs would ultimately lead to racial and/or geographic segregation. The best practice for reducing gang violence is to understand the population, provide appropriate social therapy and interventions, and manage the population based on the specific dynamics of the camp.

RECOMMENDATION NO. 16.4.

The Department of Probation should assign juveniles to Camps offering the specialized medical, psychiatric and educational services required by the minor.

RESPONSE

The Probation Department agrees with this recommendation. Evidenced-based practices have shown the critical value of quality assessments in ensuring the appropriate housing and delivery of services to incarcerated youth. The camp system is designed to provide services to the greatest range of youth within the open dorm environment. The Probation Department, working in collaboration with its county partners, provides a comprehensive assessment for all youth receiving Camp Community Placement (CCP) orders. Probation officers review court reports, court orders, criminal histories, and histories of prior detention or camp placements, community placements, and Department of Children and Family Services databases.

Additionally, the Probation Department reviews Department of Public and Social Services databases to ensure Medi-Cal coverage for youth upon their transition to the community. Assessment deputies administer the Los Angeles Risk and Resiliency Check-up (LARRC) to all youth, providing a validated measure of the youths' criminogenic factors, and appropriate evidenced-based interventions.

LACOE has provided the Probation Department with an in-house Senior Program Specialist at the Assessment Center to act as a liaison with the assessment team. The liaison provides insight into the educational needs of youth, the level of special education interventions required, and the credit status of youth awaiting camp assignment. The Department of Mental Health (DMH) has allocated a team of clinicians working out of the Assessment Office. The clinicians provide insight into the mental health needs of youth with camp orders. They also identify the levels of substance abuse intervention appropriate to those youth in need. Additionally, the clinicians identify which camps can provide the appropriate services to specific youth, including psychiatric monitoring of medication. While camps strive to provide the most services to the largest spectrum of those youth having CCP orders, some youth exhibit needs that cannot be met at camp. Typically, these youth will have profound medical or mental health needs requiring an alternative disposition other than open camp. Working with our partners, the Probation Department will prepare the petitions required, and provide alternatives that better meet the needs of these youth to the courts.

All camps provide substance use counseling and evidenced-based cognitive behavioral interventions. All camps also provide mandated educational services, and 10 camps provide special day class educational instruction. Camps Paige and Kilpatrick provide out-of-camp forestry work crews and sports programming, respectively. The assessment process identifies youth most appropriate to each of these locations and the specific services that they offer.

RECOMMENDATION NO. 16.5.

The Probation Department should refer all juveniles who have attempted suicide to a dedicated psychiatric facility or other Camp with mental health specialist for evaluation and treatment.

RESPONSE

The Probation Department agrees with this recommendation. Currently, the Probation Department has a suicide prevention policy in place to ensure that all youth receive the appropriate mental health evaluation and treatment. All Probation facility staff members have been trained, and receive annual refresher training in enhanced supervision protocols to proactively address self-injurious and/or suicidal behavior. All staff members are required to be aware of the various indicators of these behaviors in order to implement appropriate supervision precautions for affected minors, as well as the importance of timely referrals to DMH for initial and ongoing assessments and treatment for the youth.

The training includes an understanding as to the reasons that the environments of juvenile correctional facilities are conducive to suicidal behavior, potential pre-disposing factors to suicide, high-risk suicide periods, warning signs and symptoms, identifying suicidal minors despite the denial of risk, a review of the Probation Department's policy for suicide prevention, suicide prevention policy, the use of emergency cut down tools, and the liability issues associated with successful suicides within custodial environments.

RECOMMENDATION NO. 16.6.

The Department of Probation and Los Angeles County Office of Education should implement innovative reading programs to increase the reading decoding and comprehension levels of juveniles at all of the Camps.

RESPONSE

The Probation Department and the LACOE agree with this recommendation. This recommendation has been implemented. The following innovative reading programs are currently offered at Juvenile Camps to increase reading decoding and comprehension levels:

Achieve 3000

Achieve 3000 is a reading intervention program that not only improves students' reading levels, but also delivers content aligned with state content and common core standards. Ongoing assessments are built into the daily instructional routine, enabling continual progress monitoring and data-driven decision making.

English Language Arts Intensive Intervention: READ 180

READ 180 is a reading program designed for students whose reading achievement is below the proficient level. The goal of READ 180 is to address gaps in students' skills through the use of a computer program, literature and direct instruction in reading skills. The software component of the program aims to track and adapt to each student's progress.

Operation READ

Operation READ is a tutoring program for youth at the camps. The program goals are to build the youth's literacy skills to include reading, comprehension, writing, and spelling. Academic mentors work with the youth one-to-one and in small groups three to five hours per week to provide a variety of instructional approaches individualized to the learner.

After School Extended Learning Opportunities (ELO) Program

Students may extend their learning beyond the school day in the after-school ELO Program. This program includes a small student-to-teacher ratio. Students are offered CAHSEE Prep, GED Prep, and Language Arts intervention curriculum.

Data will be gathered during the 2013-14 school year to monitor and determine the level of implementation and effectiveness of each program. Teachers also analyze reading achievement data regularly within their Professional Learning Communities (PLCs). This analysis allows teachers to develop innovative strategies to improve students' decoding and comprehension levels.

RECOMMENDATION NO. 16.7.

The Department of Probation must aggressively reduce the staff on long-term disability and light duty unable to carry out the duties for which they were originally hired.

RESPONSE

The Probation Department agrees with this recommendation. In an effort to return staff members to work as quickly as possible, the Probation Department implemented an adaptation of the Los Angeles County Sheriff's Department's Return To Work Unit practices in November of 2011. It is a decentralized approach, which has allowed the Probation Department to successfully reduce the number the staff out on industrial or medical leave by 48% in the camps and 12% in the juvenile halls. It also allowed the Probation Department to save a total \$6.02 million in workers compensation claims. This coincides with the reduction in the RTW Caseload, and demonstrates that the Probation Department is getting employees back to work faster. These savings are occurring despite a state-wide trend of increased medical costs.

RECOMMENDATION NO. 16.8.

The Department of Probation must increase the number of cameras placed throughout the Camps to assist investigating the high percentage of injury claims resulting in long-term disability or light duty dispositions.

RESPONSE

The Probation Department agrees with this recommendation. The Probation Department is in the process of finalizing the Security Enhancement Project, which includes the installation of

cameras, microphones and panic buttons in four Probation Department facilities: Barry J. Nidorf, Central and Los Padrinos Juvenile Halls, and Challenger Memorial Youth Center (CMYC). At CMYC, surveillance equipment has been installed in dayrooms, corridors and bedrooms in the boys and girls Special Handling Units. The equipment is computer-based, and recordings are electronic so there is no need to change tapes or disks.

Officers working in the units have real time access to the system, and are responsible for monitoring the cameras and responding to intercom calls. Supervisors and directors have a higher level of access, and may view real time activity, as well as review recordings. Investigative units are able to view real time activity, and review past events, as well as export and make copies. As of July 12, 2013, the system is installed and operational at Los Padrinos and Central Juvenile Halls. It is expected that installation will be complete and the system operational at Barry J. Nidorf and CMYC by August 1, 2013. In addition, the Department will continue to seek funding to enhance the video surveillance systems for the remaining facilities.

RECOMMENDATION NO. 16.9.

The Department of Probation should increase training in self-defense and injury prevention along with setting stringent strength and fitness requirements for all new hires.

RESPONSE

The Probation Department agrees with this recommendation. Currently, all institutional staff receives Probation Department approved training in Safe Crisis Management. The training is designed to provide staff with the ability to identify and safely manage various “acting out” behaviors. The staff is trained to safely manage crisis situations using non-verbal, para-verbal, verbal, and physical intervention techniques. This intervention process is constructed on a continuum, moving from lower to higher levels of restriction or intervention, ensuring the use only of that level of intervention appropriate for the situation encountered, and preventing escalation beyond that point absent exigent circumstances supporting such action. These levels, from least to most restrictive were implemented to reduce instances of injury to youth and staff members.

In addition, the Probation Department's Risk Management section is:

1. Collaborating with the Chief Executive Office's Emergency Coordinator, Jeff Terry, to develop a Facility Emergency Coordinator Training program. It is expected that the specialized training will result in a more proactive approach to ensuring a safe and secure facility, and reducing instances of accidents. The class outline, which includes a module on general facility safety, will be certified by the state.
2. Increasing inspection of the Probation Department's 52 facilities to every 3 months, rather than annually. This allows the Risk Management Bureau to increase its presence in the facilities, and allows staff an opportunity to voice health, safety and security concerns. In turn, the Risk Management Bureau will elevate and address the concerns as necessary.

3. Conducting an inquiry in to each industrial accident claim. The inquiry serves to identify and address physical plant issues, such as cracks in sidewalks and/or other issues. The Risk Management Bureau then works with the facility, and Management Services Bureau to correct these concerns.

Attachment J

Sheriff



LEROY D. BACA, SHERIFF

County of Los Angeles
Sheriff's Department Headquarters
4700 Ramona Boulevard
Monterey Park, California 91754-2169



July 18, 2013

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
Los Angeles, California 90012

Dear Members of the Civil Grand Jury:

**RESPONSE TO THE FINAL REPORT OF THE
2012-13 LOS ANGELES COUNTY CIVIL GRAND JURY**

Attached is the Los Angeles County Sheriff's Department's (Department) response to the 2012-13 Civil Grand Jury Report recommendations. The Civil Grand Jury's areas of interest specific to the Department included: the Dual Track Career Path, training regarding the handling of mentally ill inmates, and improvements to our court lockups and station jails.

Should you have questions regarding our response, please contact Division Director Glen Dragovich at (323) 526-5191.

Sincerely,

A handwritten signature in cursive script that reads "Leroy D. Baca".

LEROY D. BACA
SHERIFF

A Tradition of Service

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – SHERIFF

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
DUAL TRACK AND TRAINING

RECOMMENDATION NO. 1.1

The Sheriff's Department leadership must counter the negative bias of Patrol officers towards those officers assigned to custody. This will also be critical if large numbers of women stay in custody positions.

RESPONSE

The Department agrees with this recommendation. It is anticipated that upon full implementation of the Dual Track Career Path, morale in both the Custody and the Patrol Divisions will improve, primarily due to the increase in opportunities for promotion and advancement into specialized units within Custody Division, and due to the significantly shorter time spent in a custody assignment by those deputies choosing to transfer to a patrol assignment.

RECOMMENDATION NO. 1.2

The Sheriff's Department in conjunction with the Board of Supervisors must come to a decision about MCJ. Many of MCJ's issues are unique to this facility. If problems at MCJ have to do with the architectural shortcomings, then funding needs to be provided to either rebuild or renovate the facility in accordance with current best practices. Different solutions may be needed for other large scale facilities like Pitchess Ranch or CRDF, as well as Court House Facilities.

RESPONSE

The Department agrees with this recommendation; a comprehensive review of the Department's current and future inmate housing needs is underway. In addition to the significant structural and design issues associated with MCJ, there is also a need for appropriate medical and mental health inmate housing.

RECOMMENDATION NO. 1.3

The Sheriff's Department should focus on keeping time spent in custody assignments to ideally no more than two years (for those wishing to go on Patrol) while increasing the learning opportunities while on custody assignment.

RESPONSE

The Department agrees with this recommendation. It is anticipated that full implementation of the Dual Track Career Path will result in a significantly shorter mandatory custody assignment for those newly hired deputies who wish to transfer to a patrol assignment. The newly created Custody Training Bureau will enhance and standardize training opportunities throughout the division, and new job rotation policies limiting the length of time a deputy can remain in a specialized assignment will afford deputies the opportunity to gain greater job knowledge, experience, and expertise.

RECOMMENDATION NO. 1.4

The Sheriff's Department must increase training for Custody positions (post Academy). But assuming limited resources, leadership should receive increased training before new deputies. The Department must look for ways to break down training into smaller units and possibly encourage through incentives or promotion consideration, having deputies seek out education on their own time. The Department needs to resolve any labor issues that may hinder this goal.

RESPONSE

The Department agrees with this recommendation. The newly established Custody Training Bureau offers a wide range of State approved classes, which address a myriad of training topics and areas. Classes are routinely updated or created to address identified issues within Custody Division. In addition, a large number of two hour Intensified Training Format (ITF) classes are taught at the facility level, negating the costs related to sending students to training off site for a full day. Custody Division policy mandates newly assigned sergeants and lieutenants attend Custody Incident Command School within the first three months of assignment to the division. The Custody Training Bureau is currently in the process of revising curriculum to formalize training for line supervisors on subjects such as handling mentally ill inmates, inmate extractions, and jail specific restraint techniques training.

RECOMMENDATION NO. 1.5

The Sheriff's Department needs to mentor and model behavior more effectively. Custody assignment is an opportunity to learn more about gangs, criminal techniques, and criminal networks outside of the jails and how to cultivate potential informants.

RESPONSE

The Department agrees with this recommendation. The Custody Training Bureau currently provides training related to jail gangs and their criminal behavior to newly graduated custody personnel during State mandated Jail Operation's School. In addition, the unit offers State certified Jail Gangs and Jail Intelligence Gathering classes on a regular basis.

RECOMMENDATION NO. 1.6

The Sheriff's Department in conjunction with the Department of Health needs to significantly increase mental health training Department-wide. The Department needs to work with other entities (Department of Mental Health, the county's e-education system, non-profits and private enterprise) to come up with ways to disseminate this training without causing positions to be backfilled while officers attend the training. Specifically, more needs to be taught relating to Post Traumatic Stress Disorder (PTSD), trauma and the behaviors that may result as well as de-escalation techniques.

RESPONSE

The Department agrees with this recommendation. In conjunction with the Department of Mental Health (DMH), the Custody Training Bureau currently provides mental health training to all newly assigned custody personnel. In addition, the Custody Training Bureau partnered with DMH to create and upload e-learning mental health training videos, which are available to personnel without having to leave their workstations. The Custody Training Bureau is currently participating in a Custody Division-wide process that is focusing on the expansion of our training curriculum and partnering with mental health professionals.

RECOMMENDATION NO. 1.7

The Sheriff's Department must provide deputies who work directly with the mentally ill extensive, specialized training. This training should emphasize recognizing, reacting to, de-escalating and preventing aggressive and hostile behavior that can occur in these settings.

RESPONSE

The Department agrees with this recommendation. The Custody Training Bureau is currently participating in a Custody Division-wide process that is focusing on the expansion of our mental health training curriculum and partnering with mental health professionals.

RECOMMENDATION NO. 1.8

The Sheriff's Department needs to use more Custody Assistants and investigate possibly contracting with private security forces for Type I facilities. It should also investigate using orderlies and specialized health care workers when dealing with mentally ill inmates.

RESPONSE

The Department generally agrees with this recommendation. For years, the Sheriff's Department has utilized Custody Assistants in Type I facilities (station jails),

incorporating them into all available positions within the scope of their classification. Some of these positions include duties such as: booking, processing, providing security, and ensuring compliance with Title 15 standards. The Sheriff's Department has studied the feasibility of further civilianization since the late 1990s, and in conjunction with employee bargaining units, continues to explore additional responsibilities for this classification.

The Sheriff's Department continues to work toward providing the best resources and care available to its inmate population. Most recently, members from Custody Division and the Department of Mental Health reviewed methods of improving the care provided to the mentally ill population. In August 2012, these Department members met with staff from Patton State Hospital to discuss means of improving our assessments, training, force, and prevention plans. Improvement has been achieved with the application of some of the information that was shared related to assessments and prevention plans. The feasibility of utilizing non-Department members to deal with the mentally ill population is not under consideration.

RESPONSE TO THE CIVIL GRAND JURY FINAL REPORT

COUNTY OF LOS ANGELES – SHERIFF

SUBJECT: 2012-2013 CIVIL GRAND JURY RECOMMENDATIONS FOR
DETENTION: ADULT FACILITIES

RECOMMENDATION NO. 15.3

The Sheriff's Department should provide Sheriff's deputies with additional training for dealing with prisoners with mental health issues as detailed in this Grand Jury's Dual Track report.

RESPONSE

The Department agrees with this recommendation. In conjunction with Department of Mental Health (DMH) personnel, the Custody Training Bureau currently provides mental health training to all newly assigned custody personnel. In addition, the unit partnered with DMH to create and upload e-learning mental health training videos, which are available to personnel without having to leave their workstations. The Custody Training Bureau is currently participating in a Custody Division-wide process that is focusing on the expansion of training curriculum and partnering with mental health professionals.

RECOMMENDATION NO. 15.5

The Sheriff's Department should take steps to insure that Courthouse facilities' video surveillance systems and cell doors that impair sightlines and visibility are upgraded.

RESPONSE

The Department agrees with this recommendation. Courthouse facilities needing video surveillance systems and retrofitting of cell doors require a feasibility proposal, as well as a proposed cost from the Department of Public Works. Facilities Planning Bureau will initiate this process.

RECOMMENDATION NO. 15.7

East Los Angeles Station – (LASD) (A32)

Padded flooring should be installed in the sobering cell and a separate telephone line should be installed for jailers.

RESPONSE

The Department agrees with this recommendation. East Los Angeles Station's proposed sobering cell does not meet the Board of State and Community Corrections requirements, due to safety concerns regarding bars. The project scope must be expanded to include the installation of a solid wall and a door with view panel, as well as padding and a fire sprinkler system. Facilities Planning Bureau will initiate this process.

RECOMMENDATION NO. 15.8

Edelman Children's Dependency Court (LASD) (A33)

This adult facility has outer doors leading to the cells that have been inoperative for the past five years. This endangers the deputies every time they remove prisoners.

RESPONSE

The Department agrees with this recommendation; however, repairs to the Children's Court are the responsibility of the State courts. Facilities Planning Bureau will make contact with the State regarding this issue.

RECOMMENDATION NO. 15.9

El Monte (Rio Hondo) Courthouse (LASD) (A34)

Cells should be painted with anti-vandalism paint, enhanced video surveillance equipment should be installed, and cell doors should be retrofitted to improve visibility.

RESPONSE

The Department agrees with this recommendation. Courthouse facilities needing video surveillance and anti-vandalism paint will be reviewed by Facilities Planning Bureau and renovations will commence when funding is available.

RECOMMENDATION NO. 15.11

Mental Health Courthouse (LASD) (A67)

This facility was well maintained for an older facility. Although 100% of the prisoner population had mental health issues, only one deputy had received more formal specialized training in mental health. All custody deputies at this and other facilities that deal with mental health issues should have such training.

RESPONSE

The Department agrees with this recommendation. Court Services Division is working with DMH to provide additional training to the personnel assigned to this court. Court supervisors have conducted a review of each employee's experience and training in order to place them in the most appropriate assignment.

RECOMMENDATION NO. 15.12

San Fernando Court (North Valley District) (LASD) (A98)

The holding cells should be painted with anti-vandalism paint and improved surveillance equipment should be installed.

RESPONSE

The Department agrees with this recommendation. Courthouse facilities needing video surveillance and anti-vandalism paint will be reviewed by Facilities Planning Bureau and renovations will commence when funding is available.

RECOMMENDATION NO. 15.13

Santa Clarita Valley Station (LASD) (A102) Adequate surveillance equipment should be installed; the video equipment for detainee-visitor visits should be repaired; and the facility should be upgraded to meet current Title 24 standards.

RESPONSE

The Department agrees with this recommendation. A plan to replace Santa Clarita Valley Station is being developed. The new facility will contain appropriate surveillance equipment, video visiting for inmate visitors, as well as meeting all Title 24 standards. A survey for solutions to the aging infrastructure has been conducted; however, implementation requires funding.



RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

Los Angeles World Trade Center
350 South Figueroa Street, Suite 188
Los Angeles, CA 90071

Telephone: (213) 253-5600
Facsimile: (213) 633-4733

July 27, 2013

To: Audit Committee

From: Richard Sanchez
Chief Information Officer

REVIEW OF BOARD POLICIES 6.100 - 6.112 - INFORMATION SECURITY

The Chief Information Office, in conjunction with County Counsel and the Information Security Steering Committee (ISSC) has reviewed Board Information Technology (IT) Security Policies 6.100 to 6.112 to address technology evolution and currency.

Some of the major revisions to highlight are: consistent use of language, newly defined terms, appropriate use of technology, further clarification of the Countywide Information Security Program, and support of recent IT capabilities in the area of mobile and portable devices (i.e., County-procured and personal), social media, and internet storage websites. These areas and the Summary of Revisions document (attached) are recommended revisions.

If you have any questions, please contact me or your staff may contact Robert Pittman, Chief Information Security Officer at 213-253-5631 or rpittman@cio.lacounty.gov.

RS:RP:pg

Attachments

c: Chief Executive Officer
Executive Officer, Board of Supervisors

**Board of Supervisors
Information Technology Security Policies # 6.100 to 6.112**

Summary of Revisions

# 6.100 – Information Technology and Security Policy	
a)	Reference section revised for the HITECH Act and other related Board Policies
b)	Defined terms added for County IT resources, County IT user, County IT security, County IT security incident, and County Department
c)	Added more specificity to complement policy with associated standards and procedures
d)	Further clarified Department IT Management/Departmental CIO (DCIO) responsibilities and duties
e)	Further clarified Departmental Information Security Officer (DISO) responsibilities and duties
f)	Further clarified Information Security Steering Committee (ISSC) responsibilities and duties
g)	Standardize language for Compliance and Policy Exceptions section
# 6.101 – Use of County Information Technology Resources (includes AUA attachment)	
a)	Reference section revised for the HIPAA and HITECH Act including related Board Policies
b)	A Definition Reference section was added
c)	Standardize language for Compliance and Policy Exceptions section
# 6.101 – Use of County Information Technology Resources – Acceptable Use Agreement	
a)	The Header was revised to include 'Annual'
b)	Reference to policies are now explicit not implicit
c)	Significant policy statements (from # 6.100 to 6.112) were replicated to underscore its criticality
d)	Item 2 (NEW) – County IT Security Reporting
e)	Item 5 – Approved Business Purpose revised for greater clarity
f)	Item 6 (NEW) – Approved Devices
g)	Item 8 – Confidentiality: inserted the word 'store'
h)	Item 11 – Internet: old section name was Public Internet
i)	Item 14 (NEW) – Public Forums
j)	Item 15 (NEW) – Internet Storage Sites
k)	California Penal Code 502(c) were amended to include paragraph (9)
l)	Signature block now utilizes newly define term of County IT user (includes/requests employee ID #, manager's title, etc.)
# 6.102 – Countywide Antivirus Security	
a)	Reference section revised for currency including other related Board Policies
b)	A Definition Reference section was added
c)	The first two statements under the Policy section are additions
d)	Standardize language for Compliance and Policy Exceptions section
# 6.103 – Countywide Computer Security Threat Responses	
a)	Reference section revised for currency including other related Board Policies
b)	A Definition Reference section was added
c)	The first two statements under the Policy section are additions
d)	Standardize language for Compliance and Policy Exceptions section
# 6.104 – Use of County Electronic Mail (e-mail) by County Employees	
a)	Reference section revised for currency including other related Board Policies
b)	A Definition Reference section was added
c)	The first two statements under the Policy section are additions
d)	Standardize language for Compliance and Policy Exceptions section
# 6.105 – Internet Usage	
a)	Reference section revised for currency
b)	A Definition Reference section was added
c)	The first two statements under the Policy section are additions
d)	(NEW) The third statement reflects using internet for business and non-business purposes
e)	(NEW) The fifth and sixth statement focuses on social media and online storage sites

**Board of Supervisors
Information Technology Security Policies # 6.100 to 6.112**

Summary of Revisions

f)	Standardize language for Compliance and Policy Exceptions section
# 6.106 – Physical Security	
a)	Reference section revised for currency
b)	A Definition Reference section was added
c)	The first two statements under the Policy section are additions
d)	Standardize language for Compliance and Policy Exceptions section
# 6.107 – Information Technology Risk Assessment	
a)	Reference section revised for currency including other related Board Policies
b)	A Definition Reference section was added
c)	The first two statements under the Policy section are additions
d)	Standardize language for Compliance and Policy Exceptions section
# 6.108 – Auditing and Compliance	
a)	Reference section revised for currency including other related Board Policies
b)	A Definition Reference section was added
c)	The first two statements under the Policy section are additions, and third statement is revised
d)	Standardize language for Compliance and Policy Exceptions section
# 6.109 – Security Incident Reporting	
a)	Reference section revised for currency including other related Board Policies
b)	A Definition Reference section was revised
c)	The first two statements under the Policy section are additions along with formatting and language revisions
d)	Standardize language for Compliance section
e)	There are no exceptions to this policy
# 6.110 – Protection of Information on Portable Computing Devices	
a)	Reference section revised for currency
b)	A Definition Reference section was revised
c)	The first two statements under the Policy section are additions
d)	(DELETED) Authorization to Place Personal and/or Confidential Information on a Portable Computing Device – this authorization request form was removed from this policy
e)	Numerous policy statements revised due to personal device(s) use
f)	Standardize language for Compliance section
g)	There are no exceptions to this policy
# 6.111 – Information Security Awareness Training	
a)	Reference section revised for currency including other related Board Policies
b)	A Definition Reference section was revised
c)	The first two statements under the Policy section are additions along with some revisions to the remaining policy statements
d)	Standardize language for Compliance and Policy Exceptions section
# 6.112 – Secure Disposition of Computing Devices	
a)	Reference section revised for currency including other related Board Policies
b)	A Definition Reference section was added
c)	The first two statements under the Policy section are additions
d)	Standardize language for Compliance section
e)	There are no exceptions to this policy



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

July 13, 2004, Board Order No. 10 – Board of Supervisors – Information Technology and Security Policies

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached thereto

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

Board of Supervisors Policy No. 9.040 – Investigations of Possible Criminal Activity Within County Government

Comprehensive Computer Data Access and Fraud Act, California Penal Code Section 502

Health Insurance Portability and Accountability Act (HIPAA) of 1996

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

- ◆ ~~Comprehensive Computer Data Access and Fraud Act, California Penal Code 502.~~

- ~~Health Insurance Portability and Accountability Act (HIPAA) of 1996~~

POLICY

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

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

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

Definitions

~~As used in this Policy, the term "County IT resources" includes, without limitation, the following items, which are owned, leased, managed, operated, or maintained by, or in the custody of, the County or non-County entities for County purposes:~~

- ~~Computing devices, including, without limitation, the following:~~
 - ~~Desktop personal computers, including, without limitation, desktop computers and thin client devices;~~
 - ~~Portable computing devices, including, without limitation, the following:~~
 - ~~Portable computers, including, without limitation, laptops and tablet computers, and mobile computers that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to County IT resources;~~

- Portable devices, including, without limitation, personal digital assistants (PDAs), digital cameras, smartphones, cell phones, pagers, and audio/video recorders; and
 - Portable storage media, including, without limitation, diskettes, tapes, DVDs, CDs, USB flash drives, memory cards, and external hard disk drives.
- Multiple user and application computers, including, without limitation, servers;
- Printing and scanning devices, including, without limitation, printers, copiers, scanners, and fax machines; and
- Network devices, including, without limitation, firewalls, routers, and switches.
- Telecommunications (e.g., wired and wireless), including, without limitation, voice and data networks, voicemail, voice over Internet Protocol (VoIP), and videoconferencing;
- Software, including, without limitation, application software and operating systems software;
- Information, including, without limitation, the following:
 - Data;
 - Documentation;
 - Electronic mail (email);
 - Personal information; and
 - Confidential information.
- Services, including, without limitation, hosted services and County internet services;
- Systems, which are an integration and/or interrelation of various components of County IT resources to provide a business solution (e.g., eCAPS)

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

As used in this policy, the term "County IT user" includes any user (e.g., County employees, contractors, subcontractors, and volunteers; and other governmental staff and private agency staff) of any County IT resources, except that the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO) may mutually determine, in writing, at any time that certain persons and/or entities (e.g., general public) shall be excluded from the definition of "County IT user".

As used in this policy, the term "County IT security" includes any security (e.g., appropriate use and protection) relating to any County IT resources.

As used in this policy, the term "County IT security incident" includes any actual or suspected adverse event (e.g., virus/worm attack, loss or disclosure of personal

information and/or confidential information, disruption of data or system integrity, and disruption or denial of availability) relating to any County IT security.

As used in this policy, the term "County Department" includes the following:

- A County department
- Any County commission, board, and office which the CISO and the CIO mutually determine, in writing, at any time shall be included in the definition of "County Department"

General

County IT resources are essential County assets that shall be appropriately protected against all forms of unauthorized access, use, disclosure, or modification. Security and controls for County IT resources shall be implemented to help ensure, without limitation:

- Privacy and confidentiality
- Information integrity, including, without limitation, data integrity
- Availability
- Accountability
- Appropriate use

Countywide County IT resources policies, standards, and procedures and countywide County IT security policies, standards, and procedures establish the minimum requirements to which County Departments shall adhere. Each County Department may, at its discretion, establish supplemental policies, standards, and procedures based on unique requirements of the County Department.

RESPONSIBILITIES

Departments, Commissions, Board and Offices

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

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

County Departments

The head of each County Department is responsible for ensuring County IT security, including, without limitation, within the County Department. Management of each County Department is responsible for organizational adherence to countywide County IT resources policies, standards, and procedures and countywide County IT security policies, standards, and procedures, as well as any additional policies, standards, and procedures established by the County Department. They shall ensure that all County IT users are made aware of those policies, standards, and procedures and that compliance is mandatory.

The head of each County Department, in consultation with the CISO, shall ensure the designation of a full-time, permanent County Department employee (Departmental Information Security Officer) to be responsible for coordinating County IT security within the County Department and the designation of a functional backup (Assistant Departmental Information Security Officer).

Chief Information Office (CIO)

The Office of the CIO will shall ensure the development of eCountywide information County IT resources technology policies, that, in addition to security will specify the appropriate use of information technology (I/T) resources for internal and external activities, e-mail and other communications as well as Internet access and use. standards, and procedures and Countywide County IT security policies, standards, and procedures. These County IT security policies shall include, without limitation, the appropriate use of County IT resources for internal and external activities (e.g., email and other communications, and Internet access and use). When approved, these policies will be published and made available to all users of County I/T resources users to ensure their awareness and compliance.

Chief Information Security Officer (CISO)

The Chief Information Security Officer CISO shall reports to the Chief Information Officer (CIO) and is responsible for the I/T Countywide Information Security Program for the County. Responsibilities include The responsibilities of the CISO include, without limitation, the following:

- Developing and maintaining the Countywide Information Security Strategy Plan; ~~for the County~~
- Chairing the Information Security Steering Committee (ISSC);
- Providing information County IT security-related technical, regulatory, and policy leadership;
- Facilitating the implementation of County information IT security policies;
- Coordinating information County IT security efforts across departmental lines boundaries organizational boundaries;
- Leading information County IT security training and education efforts; and

- Directing the Countywide Computer Emergency Response Team (CCERT).

~~Departmental Information Technology Management/CIO will:~~

County Department IT Management / Departmental Chief Information Officer

The responsibilities of IT management and the departmental chief information officer of each County Department include, without limitation, the following:

- Manage information technology assets County IT resources within the County department;

~~Be responsible for any departmental information technology and security policy~~

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

- Ensure the County Department adheres to countywide County IT security policies, standards, and procedures and any additional County IT security policies, standards, and procedures established by the County Department;
- Ensure the County Department adheres to County IT security standards and procedures approved by the ISSC;
- Ensure that County IT resources are implemented and configured to meet County IT security standards and procedures approved by the Information Security Steering Committee (ISSC).
- Ensure that systems County IT resources are maintained at current critical security patch levels; and
- Implement technology IT-based services that adhere to the intent and purpose of all information technology use and applicable County IT security policies, standards and ~~guidelines~~ procedures.

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

Departmental Information Security Officer (DISO)

The DISO shall report to the highest level of IT management or to executive management within the County Department. The responsibilities of the DISO include, without limitation, the following:

- Manage security of information technology assets County IT resources within the County department;
- Assist in the development of departmental information technology County department IT security policies;
- Regularly represent the County department at the Information Security Steering Committee (ISSC);

- Coordinate Lead the Departmental Computer Emergency Response Team (DCERT); and
- Report County IT security incidents to the CISO, as required by County IT security policies, standards, and procedures.

~~Employees and Other Authorized Users~~ County Users

~~Employees and other department authorized~~ County IT users are responsible for acknowledging and adhering to County ~~information technology use and~~ IT security policies. They are responsible for protection of County ~~information assets~~ IT resources for which they are entrusted and using them for their intended purposes. ~~Employees and authorized non~~ County IT users will be are required to sign an "Acceptable Use Agreement" as a condition of being granted access to County IT systems resources. The Acceptable Use Agreement is set forth in Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources.

Information Security Steering Committee (ISSC)

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

~~ISSC responsibilities include:~~ The responsibilities of the ISSC include, without limitation, the following:

- Assisting the CISO in developing, reviewing, and recommending ~~information~~ Countywide County IT security policies;
- Identifying and recommending industry best practices for ~~information~~ Countywide County IT security;
- Developing, reviewing, ~~and~~ recommending, and approving Countywide IT security standards, procedures and guidelines;
- Coordinating inter-departmental communication and collaboration among County departments on Countywide and County Department IT security issues; and
- Coordinating Countywide IT security education and awareness.

Compliance

County employees who violate this Policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

July 13, 2004, Board Order No. 10 - Board of Supervisors Policy – Information Technology IT and Security Policyies

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached

Comprehensive Computer Data Access and Fraud Act, California Penal Code Section 502

Health Insurance Portability and Accountability Act (HIPAA) of 1996

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

Acceptable Use Agreement (Attached)

POLICY

General

This policy is applicable to all County IT users.

Each County Department shall comply with the County IT security standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this policy.

All County IT users shall sign the Acceptable Use Agreement prior to being granted access, and annually thereafter.

Activities of County IT users may be logged/stored, are a public record, and are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time.

County IT users cannot expect any right to privacy concerning their activities related to County IT resources, including, without limitation, in anything they create, store, send, or receive using County IT resources.

County IT resources shall be used for County management approved business purposes only.

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

The County has the right to administer any and all aspects of County IT resources access and other use, including, without limitation, the right to monitor Internet, email, and data access.

Monitoring and/or investigating the access to, and use of, County IT resources by County IT users shall require approval by County management. If evidence of abuse is identified, notice shall be provided by County Department management to the Auditor-Controller's Office of County Investigations.

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

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

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

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

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

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

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

Definitions

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

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

- ~~County purchased, licensed, or developed software.~~

Access Control

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

Unless specifically authorized by County Department management or policy, access to any County IT resources and any related restricted work areas and facilities is prohibited.

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

Access control mechanisms may include, without limitation, hardware, software, storage media, policy and procedures, and physical security.

Authentication

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

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

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

Representing yourself as someone else, real or fictional, or sending information anonymously is prohibited unless specifically authorized by County ~~d~~-Department ~~m~~Management.

~~County IT information technology resource users shall be responsible for the integrity of the authentication mechanism granted to them. For example, County IT users shall not share their computer identification codes passwords, electronic cards, biometric logons, secure ID cards and/or other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, SecurID cards/tokens, biometric logons, and smartcards), with others.~~

Fixed passwords, which are used for most access authorization, shall ~~must~~ be changed at a minimum of ~~least~~ every ninety (90) days.

Data Information Integrity

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

Accessing County IT Technology Resources Remotely

Remote access to County IT ~~technology~~ resources by a County IT user shall require approval by County management. Each County IT user shall comply with, and only use equipment (e.g., County-owned computing device and personally owned computing device) that complies with, all applicable County IT resources policies, standards, and procedures, including, without limitation, antivirus software which is installed and up-to-date, operating system software and application software which are up-to-date (e.g., critical updates, security updates, and service packs), and firewall (i.e., software firewall on the computing device or hardware firewall) which is installed and up-to-date. ~~an employee or non-County employee owned equipment must be approved by department management and/or be part of an approved contract. In all cases, the equipment being used for access must be compliant with County security software requirements.~~

Privacy

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

Confidentiality

Unless specifically ~~expressly~~ authorized by County Department management or policy, ~~;~~ sending, disseminating ~~disclosing~~, or otherwise disclosing ~~disseminating~~ confidential information ~~data, protected information, or personal~~ ~~other confidential information,~~ of the County is strictly prohibited. This includes, without limitation, information that is protected under HIPAA, HITECH Act, or any other confidentiality or ~~privacy~~ legislation.

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "computing devices" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

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

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge, as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions, as well as and/or penalties both civil and criminal penalties. ~~criminal and civil.~~

Policy Exceptions

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

(See Acceptable Use Agreement)

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:

DRAFT

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

ANNUAL

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

This Agreement is required by Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, which may be consulted directly at website <http://countypolicy.co.la.ca.us/6.101.htm>.

As used in this Agreement, the term "County IT resources" includes, without limitation, computers, systems, networks, software, and data, documentation and other information, owned, leased, managed, operated, or maintained by, or in the custody of, the County or non-County entities for County purposes. The definitions of the terms "County IT resources", "County IT user", "County IT security incident", "County Department", and "computing devices" are fully set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy, which may be consulted directly at website <http://countypolicy.co.la.ca.us/6.100.htm>. The terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information, which may be consulted directly at website <http://countypolicy.co.la.ca.us/3.040.htm>.

As a County IT user, I agree to the following:

1. Computer crimes: I am aware of California Penal Code Seciton 502(c) -Comprehensive Computer Data Access and Fraud Act (set forth, in part, below attached). I shall will immediately report any suspected computer misuse or crimes to my management any suspected misuse or crimes relating to County IT resources or otherwise.
2. County IT security incident reporting: I shall notify the County Department's Help Desk and/or Departmental Information Security Officer (DISO) as soon as a County IT security incident is suspected.
3. Security access controls: I shall will not subvert or bypass any security measure or system which has been implemented to control or restrict access to County IT resources and any related restricted work areas and facilities. computers, networks, systems or data. I shall will not share

my computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, SecurID cards/tokens, biometric logons, and smartcards). (log in ID, computer access codes, account codes, ID's, etc.) or passwords.

4. Passwords: I shall not keep or maintain any unsecured record of my password(s) to access County IT resources, whether on paper, in an electronic file, or otherwise. I shall comply with all County and County Department policies relating to passwords. I shall immediately report to my management any compromise or suspected compromise of my password(s) and have the password(s) changed immediately.
5. Approved business purposes: I shall will use the County's Information Technology (IT resources)-assets including computers, networks, systems and data for County management approved business purposes only. I understand that my use of County IT resources is subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time. I understand that if my actions result in access to County IT resources from any of my personally owned computing devices (e.g., laptop, home desktop computer, personal digital assistant (PDA), smartphone, cell phone, and USB flash drives), such devices are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time.
6. Approved devices: I shall obtain written departmental management approval that includes, minimally, the Departmental Information Security Officer (DISO), for any computing device not owned or provided by the County prior to accessing and/or storing County IT resources.
7. Remote access: I understand that remote access to County IT resources shall require approval by County management. If I am authorized to remotely access County IT resources, I shall comply with, and only use equipment that complies with, all applicable County IT resources policies, standards, and procedures, including, without limitation, antivirus software which is installed and up-to-date, operating system software and application software which are up-to-date (e.g., critical updates, security updates, and service packs), and firewall (i.e., software firewall on the computing device or hardware firewall) which is installed and up-to-date.
8. Confidentiality: I shall will not access, store, or disclose to any person County program code, data, information or documentation to any individual or organization, any County IT resources (e.g., software code; business data, documentation, and other information; personal data, documentation, and other information; and confidential data, documentation, and other information), unless specifically authorized to do so by County management. the recognized information owner.
9. Computer virus and other malicious devices code: I shall will not intentionally introduce any malicious device (e.g., computer virus, spyware, and worms or malicious code), into any County IT resources. computer, network, system or data. I shall not use County IT resources to intentionally introduce any malicious device into any County IT resources or any non-County IT systems or networks. I shall will not disable, modify, or delete computer security software (e.g., antivirus software, antispymware software, firewall software, and host intrusion prevention software) on County IT resources. I shall notify the County Department's Help Desk and/or DISO as soon as any item of County IT resources is suspected of being compromised by a

malicious device, virus detection and eradication software on County computers, servers and other computing devices I am responsible for.

10. Offensive materials: I shall will not access, create, or distribute send any offensive materials, (e.g., via e-mail) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County IT resources (e.g., over County-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless it is in the performance of my assigned job duties (e.g., law enforcement). I shall report to my management any offensive materials observed or received by me on County IT resources. sexually explicit, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.
11. Internet: I understand that the Internet is public and uncensored and contains many sites that may be considered offensive in both text and images. I shall use County Internet services for County management approved business purposes only (e.g., as a research tool or for email communication). I understand that County Internet services may be filtered, but in my use of them, I may be exposed to offensive materials. I agree to hold County harmless from and against any and all liability and expense should I be inadvertently exposed to such offensive materials.
12. Email and other information: I understand that County email and other information, in either electronic or other forms, may be logged/stored, are a public record, and are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time. I shall comply with all County email use policies, standards, and procedures and use proper business etiquette when communicating over email systems.
13. Activities related to County IT resources: I understand that my activities related to County IT resources (e.g., use of email, instant messaging, blogs, electronic files, County Internet services, and County systems) may be logged/stored, are a public record, and are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time. I do not expect any right to privacy concerning my activities related to County IT resources, including, without limitation, in anything I create, store, send, or receive using County IT resources. I shall not intentionally, or through negligence, damage, interfere with the operation of, or prevent authorized access to, County IT resources and shall use County IT resources responsibly, professionally, ethically, and lawfully.
14. Public forums Internet: I shall not use County IT resources to create, exchange, publish, distribute, or disclose in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) without understanding the potential risk. I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services may be filtered but in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be inadvertently exposed to such offensive materials. I understand that my Internet

activities may be logged, are a public record, and are subject to audit and review by authorized individuals.—

15. Internet storage sites: I shall not store County information on any Internet storage site without understanding the potential risk. ~~Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will comply with County e-mail use policy and use proper business etiquette when communicating over e-mail systems.—~~
16. Copyrighted and other proprietary materials: I shall will not copy or otherwise use any copyrighted or other proprietary materials (e.g., licensed software and documentation), except as permitted by the applicable license agreement and approved by County management. ~~any licensed software or documentation except as permitted by the license agreement.—~~
17. Compliance with County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements: I shall comply with all applicable County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements relating to County IT resources. These include, without limitation, Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy, Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, and Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.
18. Disciplinary action and other actions and penalties for non-compliance: I understand that my non-compliance with any provision portion of this Agreement may result in disciplinary action and other actions (e.g., including my suspension, discharge, denial of access, and termination of contracts) as well as both civil and criminal penalties and that County may seek all possible legal redress. ~~service, cancellation of contracts or both civil and criminal penalties~~

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

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

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

- (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongly control or obtain money, property, or data.
- (2) Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or

external to a computer, computer system, or computer network.

- (3) Knowingly and without permission uses or causes to be used computer services.
- (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
- (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.
- (9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

County IT User's Name

County IT User's Signature

County IT User's Employee/ID Number

Date

Manager's Name

Manager's Signature

Manager's Title

Date

~~Employee's Name~~ ~~Employee's Signature~~ ~~Date~~

~~Manager's Name~~ ~~Manager's Signature~~ ~~Date~~

DRAFT



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

To establish an antivirus security policy for the protection of all County **I**nformation **T**echnology (**IT**) resources.

REFERENCE

July 13, 2004, Board Order **No.** 10 - Board of Supervisors Policy – Information Technology **IT** and Security Policies

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

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached thereto

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

POLICY

This policy is applicable to all County IT users.

Each County Department shall comply with the County IT security standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this policy.

Each **C**ounty **D**ePARTMENT shall provide County-approved real-time virus protection for all County hardware/software environments to mitigate risk to County **IT resources** data, devices, and networks.

Antivirus software shall be configured to actively scan all files received by the **a**

computing device.

Each County Department shall ensure that computer security software (e.g., antivirus software, antispyware software, firewall software, and host intrusion prevention software) is updated when a new detection definition file, detection engine, software update (e.g., service packs and upgrades), and/or software version release, as applicable, is available, and when hardware/software compatibility is confirmed.~~antivirus software is updated when a new antivirus definition/software release is available and when hardware/software compatibility is confirmed.~~

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

Each County Department ~~shall~~ must comply with the requirements of the Countywide Computer Emergency Response Team (CCERT) policy in the notification of County IT security incidents ~~credible computer threat events.~~

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

Remote access to County IT resources by a County IT user shall require approval by County management. The County IT user shall comply with, and only use equipment (e.g., County-owned computing device and personally owned computing device) that complies with, all applicable County IT resources policies, standards, and procedures, including, without limitation, antivirus software which is installed and up-to-date, operating system software and application software which are up-to-date (e.g., critical updates, security updates, and service packs), and firewall (i.e., software firewall on the computing device or hardware firewall) which is installed and up-to-date.

County employees and other persons are prohibited from intentionally introducing any malicious device (e.g., computer virus, spyware, worm, and malicious code), into any County IT resources. Further, County employees and other persons are prohibited from using County IT resources to intentionally introduce any malicious device into any County IT resources or any non-County IT systems or networks.

County employees and other persons are prohibited from disabling, modifying, or deleting computer security software (e.g., antivirus software, antispyware software, firewall software, and host intrusion prevention software) on County IT resources.

Each County IT user is responsible for notifying the County Department's Help Desk and/or Departmental Information Security Officer (DISO) as soon as any item of County IT resources is suspected of being compromised by a malicious device.

~~Any employee or authorized user who telecommutes or is granted remote access shall utilize equipment that contains current County-approved anti-virus software and shall~~

~~adhere to County hardware/software protection standards and procedures that are defined for the County and the authorizing department.~~

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

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

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

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "computing devices" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security incident" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

Compliance

County Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge, as well as civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions, as well as and/or penalties both civil and criminal penalties and civil.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.103	Countywide Computer Security Threat Responses	07/13/04

PURPOSE

The purpose of this Policy is to define the County's responsibility in responding to ~~countywide computer~~ security threats affecting the confidentiality, integrity, and/or availability and/or integrity of County ~~computerized data, and/or information processing information technology (IT)~~ resources.

REFERENCE

July 13, 2004, Board Order No. 10 - Board of Supervisors Policy – Information Technology and Security Policyies.

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

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached thereto

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

Board of Supervisors Policy No. 9.040 – Investigations of Possible Criminal Activity Within County Government

POLICY

Each County Department shall comply with the County IT security standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this Policy.

The County shall establish a Countywide Computer Emergency Response Team (CCERT). The CCERT will be led by the Chief Information Security Officer (CISO) and

will shall consist of representatives from all County departments. CCERT will shall communicate security information, guidelines for notification processes, identify potential security risks, and coordinate responses to thwart, mitigate or eliminate a countywide computer security threats to County IT resources.

Upon the activation of CCERT by the CISO, all Departmental Information Security Officers (DISOs), Assistant DISOs, and other CCERT representatives shall report directly to the CISO for the duration of the CCERT activation.

Each County department shall establish a Departmental Computer Emergency Response Team (DCERT) that is led by the Departmental Information Security Officer (DISO) and has the responsibility for responding to and/or coordinating computer the response to security threats events to County IT resources within their organization the County department. Representatives from each DCERT shall also be active participants in CCERT.

Upon the activation of a County department's DCERT by the DISO, all DCERT representatives shall report directly to the DISO for the duration of the DCERT activation.

Each County department shall establish and implement Departmental Computer Emergency Response Procedures. The DCERT shall inform the CCERT, as early as possible, of computer security threat events that could adversely impact countywide computer systems and/or data to County IT resources.

Each County department shall develop a notification process, to ensure management notification within their County department and to the CCERT, in response to computer County security events incidents.

The CCERT and DCERTs have the responsibility to take necessary corrective action to remediate a computer County IT security threat incidents.

Each department shall provide CCERT with after-hours contact information, including without limitation, after-hours, for their its primary and secondary CCERT representatives (e.g., DISO and Assistant DISO) and immediately notify CCERT of any changes to that information. Each County department shall maintain current contact information for all personnel who are important for the responsible response to security threats for managing to County I/T resources to be utilized to remediate and/or the remediation of County IT security threats incidents.

Each County departments shall provide its primary and secondary members CCERT representatives with adequate portable communication devices. (e.g., cell phone, and pager, etc).

In instances where violation of any law may have occurred, proper notifications will be made in accordance with existing County policies.

Definition Reference

As used in this Policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this Policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this Policy, the term "County IT security incident" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this Policy, the term "County department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

Compliance

County employees who violate this Policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:

DRAFT



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.104	Use of Electronic Mail (e-mail) by County Employees	07/13/04

PURPOSE

To ensure that all County e-mail communications ~~are used in accordance with applicable laws and County Use of Information Technology Policies~~ using County information technology (IT) resources are in accordance with County IT resources polices, County IT security policies, and applicable law. This policy also requires that electronic mail systems County email systems/services shall be secured to prevent unauthorized access, to prevent unintended loss or malicious destruction of data and other information, and to provide for their integrity and availability of such systems/services.

REFERENCE

July 13, 2004, Board Order No. 10 - Board of Supervisors Policy – Information Technology and Security Policies

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

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached thereto

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

POLICY

This policy is applicable to all County IT users.

Each County Department shall comply with the County IT security standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this policy.

E-mail is provided as a County resource for conducting County business.

Access to County e-mail services is a privilege that may be wholly or partially restricted without prior notice or without consent of the user.

The County has the right to administer any and all aspects of access to, and use of, County email systems/services. Access to County email systems/services is a privilege that may be wholly or partially restricted without prior notice or without consent of the County IT user.

All e-mail ~~messages~~ communications using County IT resources are the property of the County. All email communications using County IT resources may be logged/stored, are a public record, and are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons as directed by County management. County IT users cannot expect a right to privacy when using County email systems/services. ~~by authorized County personnel. Staff cannot expect a right to privacy when using the County e-mail system .~~

~~All County e-mail is subject to audit and periodic unannounced review by authorized individuals as directed by County management. The County reserves the right to access and view all electronic mail messages for any business purpose.~~

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

County departments shall take appropriate steps to protect all e-mail servers County email systems/services from various types of security threats.

~~Internet based e-mail services shall not be accessed using County information technology resources except for County purposes.~~ County Internet services shall be used for County management approved business purposes only.

~~E-mail retention must comply with legal requirements, but must be minimized to conserve information technology~~ All email communications using County IT resources shall be retained in compliance with legal requirements, but retention shall be minimized

to conserve County IT resources and prevent risk of unauthorized disclosure.

Unless specifically authorized by County Department management or policy, sending, disseminating, or otherwise disclosing confidential information or personal information, is strictly prohibited. This includes, without limitation, information that is protected under HIPAA, HITECH Act, or any other confidentiality or privacy legislation.

~~Encryption of e-mail may be appropriate or required in some instances to secure the contents of an e-mail message~~ email communications using County IT resources may be appropriate or required in some instances to secure the contents of email communications.

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

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

Compliance

County employees who violate this Policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-County employees including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties ~~and/or penalties both criminal and civil.~~

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (~~CI~~)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.105	Internet Usage Policy	07/13/04

PURPOSE

To establish a County Information Technology (IT) countywide security policy for acceptable use of the Internet utilizing County IT information technology resources.

REFERENCE

July 13, 2004, Board Order No. 10 - Board of Supervisors Policy – Information Technology and Security Policy.

July 13, 2004, Board Order No. 10 – Board of Supervisors – Information Technology and Security Policies

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

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached thereto

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

POLICY

This policy is applicable to all County IT users, ~~employees, contractors, sub-contractors, volunteers and other governmental agency staff who have access to the Internet through use of County resources.~~

Each County Department shall comply with the County IT security standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this policy.

County IT resources, including, without limitation, County Internet services, shall be used for business and non-business purposes when in compliance with the following criteria, when the use:

- Must in no way undermine the use of County IT resources for official County purposes
- Must not hinder productivity or interfere with a County IT user's obligation to perform their duties in a timely manner
- Neither expresses nor implies sponsorship or endorsement by the County. Any posting to public forums (e.g., newsgroups, chat rooms), or any transmittal of County electronic mail through the Internet for non-business use must include a disclaimer that the views are those of the employee/user and not the County of Los Angeles
- Shall not result in personal gain (e.g., outside business activities, items for sale)

Unless specifically authorized by County Department management or policy, sending, disseminating, or otherwise disclosing confidential information or personal information, is strictly prohibited. This includes, without limitation, information that is protected under HIPAA, HITECH Act, or any other confidentiality or privacy legislation.

No County IT user shall use County IT resources to create, exchange, publish, or distribute in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) without understanding the potential risk.

No County IT user shall store County information on any Internet storage site without understanding the potential risk.

No County IT user of County Internet services shall intentionally or through negligence damage, interfere with the operation of, or prevent authorized access to County IT resources.

Access to County Internet services shall require approval by County management. County IT users authorized to access County Internet services shall not allow another person to access County Internet services using their account.

Access to County Internet services is provided to a person at the discretion of each County Department.

The County has the right to administer any and all aspects of access to, and use of, County Internet services, including, without limitation, monitoring sites visited by County IT users on the Internet, monitoring chat groups and newsgroups, reviewing materials downloaded from or uploaded to the Internet by County IT users, and limiting access only to those sites required to conduct County business.

Monitoring and/or investigating the access to, and use of, County IT resources by County IT users shall require approval by County management. If evidence of abuse is identified, notice shall be provided by County Department management to the Auditor-Controller's Office of County Investigations.

The use of County Internet services for personal gain, gaining unlawful access or attempting unlawful access to non-County IT resources, or activities that are detrimental to the County are prohibited.

The following inappropriate use of County Internet services are examples only and are not intended to limit the scope of potential use violations:

- Downloading or distributing software unless approved by County management
- Downloading or distributing material in violation of copyright laws (e.g., movies, music, software, and books)
- Downloading or distributing pornography or other sexually explicit materials
- Any activities that could be construed as a violation of law
- Posting or transmitting scams (e.g., pyramid schemes and "make-money-fast" schemes) to others
- Posting or transmitting any message or material which is libelous or defamatory
- Running a private business or web site
- Posting or transmitting to unauthorized persons any material deemed to be confidential information or personal information
- Participating in partisan political activities

- Attempting an unauthorized access to the account of another person or group on the Internet, or attempting to penetrate beyond County security measures or security measures taken by others connected to the Internet, regardless of whether or not such intrusion results in corruption or loss of data or other information
- Knowingly or carelessly distributing malicious code to or from County IT resources

~~County information technology resources, including Internet access, are established to be used for County business purposes.~~

~~No County Internet user shall intentionally or through negligence damage, interfere with the operation of, or prevent authorized access to County information technology resources.~~

~~Authorized users shall not allow another user to access the Internet using their authorized account.~~

~~Internet access is provided to the end user at the discretion of each County department.~~

~~The County has the right to administer any and all aspects of Internet access and use including, but not limited to: monitoring sites visited by employees on the Internet, monitoring chat groups and newsgroups, and reviewing materials downloaded from or uploaded to the Internet by users and limiting access only to those sites required to conduct County business.~~

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

~~It is prohibited to use County provided Internet access for personal gain, gaining or attempting unlawful access into information technology resources, or activities that are detrimental to the County.~~

~~The following inappropriate use of Internet activities are examples only and are not intended to limit the scope of potential Internet use violations:~~

- ~~Using the County's Internet services for the unauthorized downloading of software or file sharing software that is not specifically used for conducting County business.~~
- ~~Using the County's Internet services for downloading or distributing material in violation of copyright laws (i.e., movies, music, software, books, etc.).~~
- ~~Using the County's Internet services for downloading or distributing pornography or other sexually explicit materials.~~
- ~~Using the County's Internet services for any activities that could be construed as a violation of National/Homeland Security laws.~~
- ~~Using the County's Internet services to post scams such as pyramid schemes or "make money fast" schemes to others via the Internet.~~
- ~~Using the County's Internet services to post or transmit any message or material which is libelous, defamatory, or which discloses private or personal matters concerning any person or group.~~
- ~~Using County Internet services for running a private business or web site.~~
- ~~Using the County's Internet services to post or transmit to unauthorized individuals any material deemed to be private, proprietary, or confidential information.~~
- ~~Attempting an unauthorized access to the account of another individual or group on the Internet, or attempting to penetrate beyond County security measures or security measures taken by others connected to the Internet, regardless of whether or not such intrusion results in corruption or loss of data.~~
- ~~Knowingly or carelessly distributing malicious code to or from County information technology resources.~~
- ~~Using the County's Internet services to participate in partisan political activities.~~

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

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

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge, as well as civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and/or other actions, as well as penalties both civil and criminal penalties. and civil.

Policy Exceptions

Requests for exceptions to this Board of Supervisors (Board) policy shall must be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approved by the Board of Supervisors. Departments requesting exceptions should provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the

exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the department, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall will review such requests, confer with the requesting County Department, and place the matter on the Board's agenda along with a recommendation for Board action.

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:

DRAFT



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.106	Physical Security	07/13/04

PURPOSE

To establish a countywide County Information (IT) security policy to ensure that County IT information technology resources are protected by physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

REFERENCE

July 13, 2004, Board Order No. 10 - Board of Supervisors Policy – Information Technology and Security Policies.

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

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached thereto

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

POLICY

This policy is applicable to all County IT users.

Each County Department shall comply with the County IT security standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this policy.

Facility Security Plan

Each County Department is required to have a "Facility Security Plan", which shall include, without limitation, measures to safeguard County IT Information Technology resources. The plan shall describe ways in which all County IT Information Technology resources shall be protected from, without limitation, physical tampering, damage, theft, or unauthorized physical access.

Proper Identification

Access to areas containing confidential sensitive information or personal information shall must be physically restricted. Each person All individuals in these areas shall must wear an identification badge on their outer garments, so that both the picture and information on the badge are clearly visible.

Access to Restricted IT Areas

Restricted IT I/T areas including without limitation, data centers, computer rooms, telephone closets, network router and hub rooms, voicemail system rooms, and similar areas containing County IT I/T resources. All access to these areas shall require authorization by County management and shall must be appropriately authorized and restricted.

Physical Security Controls

A County IT user is considered a custodian for the particular assigned County IT resources. If an item is damaged, lost, stolen, borrowed, or otherwise unavailable for normal business activities, a custodian shall promptly inform the involved County Department manager.

County IT resources containing confidential information or personal information located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access.

If feasible, County IT resources owned by County shall be marked with some form of identification that clearly indicates it is the property of the County of Los Angeles.

Each County IT user is responsible for notifying the County Department's Help Desk and/or Departmental Information Security Officer (DISO) as soon as a County IT security incident is suspected.

Equipment Control

The assigned user of I/T resource is considered the custodian for the resource. If the item has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal

~~business activities, the custodian must promptly inform the involved department manager.~~

~~Sensitive I/T resources located in unsecured areas should be secured to prevent physical tampering, damage, theft, or unauthorized physical access.~~

~~When feasible, I/T equipment must be marked with some form of identification that clearly indicates it is the property of the County of Los Angeles.~~

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security incident" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

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

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge, as well as both civil and criminal penalties. Non-County employees, including without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions, as well as and/or penalties both civil and criminal penalties. ~~and civil.~~

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.107	Information Technology Risk Assessment	07/13/04

PURPOSE

To ensure the performance of periodic Information Technology (IT) countywide and departmental information security risk assessments County departments for the purpose of identifying security threats to, and security determining areas of vulnerabilities within, County IT resources and to initiating appropriate remediation.

REFERENCE

July 13, 2004, Board Order No. 10 - Board of Supervisors Policy – Information Technology and Security Policies

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

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached thereto

POLICY

Each County Department shall comply with the County IT security standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this policy.

Each County Department shall periodically conduct and document an IT risk assessment in accordance with Auditor-Controller (A-C) requirements, which are included in the annual/biennial A-C Internal Control Certification Program (ICCP) procedures.

IT Security risk assessments are is a mandatory and activity, which encompasses information gathering, analysis, and determination of security vulnerabilities within the County IT resources, including without limitation, County's hardware and software environments, and IT information technology (I/T) business business practices.

IT Security risk assessments are is necessary to analyze and mitigate security threats to the County IT resources, information technology assets, which may come from any source, including without limitation, natural disasters, disgruntled County employees, hackers, the Internet, and equipment or service malfunction or breakdown.

IT Security risk assessments shall be conducted on all County IT resources, including without limitation, ~~information systems including applications, servers, networks, and any process or procedure by which~~ the County IT resources these systems are utilized and maintained. IT risk assessments shall also be performed on each facility that houses County IT ~~information technology resources~~.

An IT risk assessment program shall include without limitation, an inventory of County IT resources; review of County IT I/T assets, review of I/T security policies, standards, and procedures; assessments and prioritization of data security threats to, and security vulnerabilities within, County IT resources; and implementation of safeguards to mitigate identified security threats to, and security vulnerabilities within, County IT resources.

~~County departments shall periodically conduct and document an information technology risk assessment in accordance with Auditor-Controller requirements.~~

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

Compliance

County employees who violate ~~departments must develop written procedures to comply with this policy~~ may be subject to appropriate disciplinary action up to and including discharge, as well as both civil and criminal penalties. Non-County employees including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions, as well as both

civil and criminal penalties. Review and remediation of risk assessment findings is the responsibility of each department.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.108	Auditing and Compliance	07/13/04

PURPOSE

~~The purpose of this policy is to establish the requirement for all information technology resources in the County to be audited on a periodic basis to ensure compliance with the information technology use and security policies.~~

To ensure that County information technology (IT) resources are periodically audited for compliance with County IT resources policies, standards, and procedures and County IT security policies, standards, and procedures.

REFERENCE

July 13, 2004, Board Order No. 10 – Board of Supervisors – Information Technology and Security Policyies

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

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached thereto

POLICY

~~The Los Angeles County Auditor-Controller shall conduct or coordinate an audit of every department's compliance to County I/T use and security policies, standards and guidelines. Audits shall be conducted for each department as scheduled by the Office of the Auditor-Controller.~~

~~Each County department shall be responsible for assisting the County Auditor-Controller in conducting a security policy audit of information technology resources.~~

~~As used in this policy, the term “County Department” shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.~~

This policy is applicable to all County IT users.

Each County Department shall comply with the County IT security standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this policy.

The Auditor-Controller (A-C) shall conduct or coordinate an audit of every County Department’s compliance with County IT resources policies, standards, and procedures, and County IT security policies, standards, and procedures. Audits shall be prioritized and scheduled based on risk by the A-C. To facilitate the audit process, each County Department shall:

- Properly complete the annual Chief Information Office’s Business Automation Planning (BAP) security questionnaire.
- Properly conduct and document IT risk assessments in accordance with A-C requirements as required by Board of Supervisors Policy No. 6.107 – Information Technology Risk Assessment.

Definition Reference

As used in this Policy, the term “County IT resources” shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this Policy, the term “County IT user” shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this Policy, the term “County IT security” shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

Compliance

~~County departments that have been audited must develop a written response that includes a plan to remediate any deficiencies found during the audit. Review and remediation of the audit findings is the responsibility of each department.~~

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and

other actions as well as both civil and criminal penalties.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

May 8, 2007, [Board Order No. 26](#) – [Board of Supervisors – Information Security Policies](#)

Board of Supervisors [Policy No. 6.100](#) – Information Technology and Security Policy

Board of Supervisors [Policy No. 6.101](#) – Use of County Information Technology Resources, [including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources \(Acceptable Use Agreement\), attached thereto](#)

Board of Supervisors [Policy No. 6.103](#) – Countywide Computer Security Threat Responses

Board of Supervisors [Policy No. 6.110](#) – Protection of Information on Portable Computing Devices

Board of Supervisors [Policy No. 3.040](#) – General Records Retention and Protection of Records Containing Personal and Confidential Information

[Board of Supervisors Policy No. 9.040](#) – Investigations of Possible Criminal Activity Within County Government

Health Insurance Portability and Accountability Act (HIPAA) of 1996

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

POLICY

This policy is applicable to all County IT users.

Each County Department shall comply with the County IT security standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this policy.

All County information technology (IT)-related security incidents shall (i.e., virus/worm attacks, actual or suspected loss or disclosure of personal and/or confidential information, etc.) ~~must~~ be reported by the Departmental Information Security Officer (DISO) to the Chief Information Security Officer (CISO), as required by County IT security policies, standards, and procedures, in a timely manner to minimize the risk to the County, its employees and assets, and other persons/entities. ~~to the applicable designated County offices in a timely manner to minimize the risk to the County, its employees and assets, and other persons/entities.~~ The County department that receives a report of a County IT security incident shall ~~an incident must~~ coordinate the information gathering and documenting process and collaborate with other affected County Departments to identify and implement a resolution or incident mitigation action (i.e., notification of unauthorized disclosure of personal information and/or confidential information to the affected employee and/or other person/entity).

The Chief Information Office shall immediately report to the Board of Supervisors (Board) County IT security incidents that involve unsecured confidential information or unsecured personal information, and other incidents as determined by the CISO.

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

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

responsibilities for the Auditor-Controller.

Each County IT user is responsible for notifying the County Department's Help Desk and/or DISO as soon as a County IT security incident is suspected.

Chief Information Security Officer (CISO)

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

- Virus or worm outbreaks that infect at least fifty (50) ~~ten (10)~~ IT computing devices (i.e., desktop and laptop computers, personal digital assistants (PDA, etc.)
- Malicious attacks on telecommunications IT networks
- Web page defacements
- Actual or suspected loss or disclosure of personal information and/or confidential information
- Lost or stolen computing devices containing personal information and/or confidential information Loss of County supplied portable computing devices (i.e., laptops, PDAs removable storage devices, etc.)

Chief HIPAA Privacy Officer (CHPO)

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

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

Office of County Investigations (OCI)

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

- System breaches from internal or external sources

- Lost or stolen computing devices containing personal information and/or confidential information and data
- Inappropriate non-work related data information, which may include, without limitation, pornography, music, and videos
- Actual or suspected loss or disclosure of personal information and/or confidential information

Chief Information Office (CIO)

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

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

Definition Reference

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

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "computing devices" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "telecommunications" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security incident" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

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

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge, as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions, as well as both civil and criminal penalties. ~~and/or penalties both criminal and civil.~~

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007

Reissue Date:

Sunset Review Date: May 8, 2011

Sunset Review Date:

DRAFT



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.110	Protection of Information on Portable Computing Devices	05/08/07

PURPOSE

To establish a policy regarding the protection of personal information and/or confidential information used or maintained by the County that resides on any portable computing devices, whether or not the devices are owned or provided by the County.

REFERENCE

May 8, 2007, [Board Order No. 26 – Board of Supervisors – Information Security Polices](#)

Board of Supervisors [Policy No. 6.100](#) – Information Technology and Security Policy

Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement), attached thereto

Board of Supervisors [Policy No. 6.109](#) – Security Incident Reporting

~~Authorization to Place Personal and/or Confidential Information on a Portable Computing Device (Attached)~~

Board of Supervisors [Policy No. 3.040](#) – General Records Retention and Protection of Records Containing Personal and Confidential Information

[Health Insurance Portability and Accountability Act \(HIPAA\) OF 1996](#)

[Health Information Technology for Economic and Clinical Health \(HITECH\) Act of 2009](#)

POLICY

This policy is applicable to all County IT users, departments, employees, contractors, subcontractors, volunteers and other governmental and private agency staff who use portable computing devices in support of County business.

Each County Department shall comply with the County IT security standards and procedures set forth by the Information Security Steering Committee (ISSC) in support of this policy.

Definition Reference

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

Placing Personal and/or Confidential Information On Portable Computing Devices

The County prohibits the unnecessary placement (download or input) of personal and/or confidential information on portable computing devices. However, users who in the course of County business must place personal and/or confidential information on portable computing devices must be made aware of the risks involved and impact to the affected person/entities in the event of actual or suspected loss or disclosure of personal and/or confidential information. If personal and/or confidential information is placed on a portable computing device, every effort must be taken, including, without limitation, physical controls to protect the information from unauthorized access and, without exception, the information must be encrypted. Additionally, a written authorization signed by a designated member of departmental management must provide written approval for the particular personal and/or confidential information to be placed on a portable computing device. The recipient (person using the portable computing device) must also sign the authorization indicating acceptance of the information and acknowledge his/her understanding of his/her responsibility to protect the information. The authorization must be reviewed and renewed, at a minimum, annually. In the event the portable computing device is lost or stolen, the department must be able to recreate the personal and/or confidential information with 100 percent accuracy and must be able to provide notification to the affected persons/entities.

Full Encryption of All Information on all Portable Computing Devices

Security measures must be employed by all County departments to safeguard all personal and/or confidential information on all portable computing devices. All County-owned or provided portable computers (e.g., laptops and tablet computers) must at all times have automatic full disk encryption that does not require user intervention nor

~~allow user choice to implement. If personal and/or confidential information is placed on any portable computing devices, all such information must be encrypted while on those portable computing devices.~~

~~Portable computing devices include, without limitation, the following:~~

- ~~• Portable computers, such as laptops and tablet computers~~
- ~~• Portable devices, such as personal digital assistants (PDA), digital cameras, portable phones, and pagers~~
- ~~• Portable storage media, such as diskettes, tapes, CDs, zip disks, DVDs, flash memory/drives, and USB drives~~

~~If personal and/or confidential information is stored on a portable computing device, it is the department's responsibility to ensure that the portable computing device supports department approved data encryption software and that all information is encrypted that resides on this vehicle.~~

~~Personal and/or Confidential Information~~

~~When it is determined that personal and/or confidential information must be placed on a portable computing device, every effort should be taken to minimize the amount of information required. Additionally, if possible, information should be abbreviated to limit exposure (e.g., last 4 digits of the social security number).~~

~~Actions Required In the Event of Actual or Suspected Loss or Disclosure~~

~~Any actual or suspected loss or disclosure of personal and/or confidential information must be reported under Board of Supervisors [Policy 6.109](#), Security Incident Reporting. In all cases, every attempt must be made to assess the impact of storing, and to mitigate the risk to, personal and/or confidential information on all portable computing devices.~~

A) Portable Computing Devices and Information

All portable computing devices that access and/or store County IT resources must comply with all applicable County IT resources policies, standards, and procedures.

The County prohibits the unnecessary placement (download or input) of personal information and/or confidential information on portable computing devices. However, County IT users who in the course of County business must place personal information and/or confidential information on portable computing devices shall be made aware of the risks involved and impact to the affected person/entities in the event of actual or suspected loss or disclosure of personal information and/or confidential information.

If personal information and/or confidential information are placed/stored on a portable computing device, every effort shall be taken, including, without limitation, physical controls, to protect the information from unauthorized access and, without exception, the information must be encrypted.

A County IT user who intends to use any portable computing device not owned or provided by the County to access and/or store County IT resources is required to obtain prior written departmental management approval that includes, minimally, the Departmental Information Security Officer (DISO).

B) Protection Requirements for Stored Information

County Departments must safeguard all personal information and/or confidential information on all portable computing devices.

All portable computers shall at all times have automatic full disk, volume, or file/folder encryption that does not require user intervention nor allow user choice to implement or modify in order to ensure all personal information and/or all confidential information is encrypted.

If personal information and/or confidential information are placed/stored on any portable computing device other than a portable computer, all such information shall be encrypted, unless not feasible and compensating controls that have been approved by the DISO are implemented.

Each County Department shall ensure that, in the event the portable computing device is lost or stolen and the stored data is not encrypted, the County Department shall be able to recreate the personal information and/or confidential information with 100 percent accuracy and shall be able to provide notification to the affected persons/entities.

C) Limit Exposure of Stored Information

When it is determined that personal information and/or confidential information needs to be placed/stored on a portable computing device, every effort should be taken to minimize the amount of information required. Additionally, if feasible, such information shall be abbreviated to limit exposure (e.g., last 4 digits of a Social Security number).

D) Actions Required In the Event of Actual or Suspected Loss or Disclosure

Any actual or suspected loss or disclosure of personal information and/or confidential information shall be reported under Board of Supervisors Policy No. 6.109 – Security Incident Reporting. In all cases, every attempt shall be made to assess the impact of storing, and to mitigate the risk to, personal information and/or confidential information

on all portable computing devices.

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "portable computing devices" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "portable computers" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

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

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge, as well as civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions, as well as both civil and criminal penalties. ~~/or penalties both criminal and civil.~~

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007

Sunset Review Date: May 8, 2011

Reissue Date:

Sunset Review Date:

DRAFT



Authorization to Place Personal and/or Confidential Information on a Portable Computing Device

Department Name _____

This Authorization to place (download or input) personal and/or confidential information on a portable computing device (portable computer, portable device, or portable storage media) must be completed for each initial placement (download or input) of the information to each device and be signed by the user of the portable computing device and designated department management in accordance with Board of Supervisors Policy 6.110 – Protection of Information on Portable Computing Devices and Board of Supervisors Policy 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information (Note – Policy 3.040 is applicable only for the purpose of providing the definitions of “personal information” and “confidential information”, as referenced in Policy 6.110). However, if the personal and/or confidential information is downloaded from a particular application system to a particular portable computing device, then this Authorization must be completed only for the initial placement (download) of the information on such device, regardless of how often the information is downloaded to such device.

For each initial placement of personal and/or confidential information on each portable computing device, the following steps are required:

1. Provide a description of the portable computing device as indicated below
2. Specify the information to be placed on such device and related information as indicated below
3. Establish an exact copy of the information, preferably on a department computer, to allow for 100% accurate re-creation and audit of the information
4. Encrypt the information during the entire time that it resides on the portable computing device
5. Maintain physical security over the portable computing device during the entire time that the information resides on the device (e.g., the user must maintain physical possession of the device or keep the device secure when unattended)
6. User signature
7. Department management signature

Portable Computing Device Description:

Device type (e.g., laptop, PDA, USB drive, etc): _____

Device serial number: _____

Property number (if County property): _____

Name of encryption software installed: _____

Operating system: _____

Information Being Placed on the Portable Computing Device:

Purpose of placement: _____

Application system name (if applicable): _____

Personal and/or confidential information fields: _____

User Agreement and Acknowledgement:

I have read and agree to fully comply with Board of Supervisors Policy 6.110 – Protection of Information on Portable Computing Devices and Board of Supervisors Policy 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information (Note – Policy 3.040 is applicable only for the purpose of providing the definitions of “personal information” and “confidential information”, as referenced in Policy 6.110). I agree to fully comply with all County requirements and directions concerning the above portable computing device and personal and/or confidential information.

Name: _____ Date: _____

Signature: _____

Department Approval:

Print Name: _____ Title: _____

Signature: _____



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.111	Information Security Awareness Training	05/08/07

PURPOSE

To ensure that the appropriate level of information security awareness training is provided to all ~~users (County employees, contractors, sub-contractors, volunteers and other governmental and private agency staff)~~ of County information technology (IT) users. resources.

REFERENCE

May 8, 1007, [Board Order No. 26 – Board of Supervisors – Information Security Policies](#)

Board of Supervisors [Policy No. 6.100](#) – Information Technology and Security Policy

[Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources \(Acceptable Use Agreement\), attached thereto](#)

Board of Supervisors [Policy No. 3.040](#) – General Records Retention and Protection of Records Containing Personal and Confidential Information

POLICY

~~Effective information security programs must include user information security awareness training as well as training in the handling and protection of personal and/or confidential information and in the user's responsibility to notify County department management in the event of actual or suspected loss or disclosure of personal and/or confidential information. Training must begin with employee orientation and must be conducted on a periodic basis throughout the person's term of~~

employment with the County.

This policy is applicable to all County IT users.

Each County Department shall comply with the County IT security standards and procedures set forth by the Information Security Steering Committee (ISSC) in support of this policy.

The Chief Information Office shall facilitate and coordinate with County Departments to establish and maintain a countywide information security awareness training program.

Information security programs at County Departments shall include, without limitation, information security awareness training which includes, without limitation, training in the handling and protection of personal information and/or confidential information and in a County IT user's responsibility to notify County Department management in the event of actual or suspected loss or disclosure of personal information and/or confidential information. For County employees, training shall begin with County employee orientation and shall be conducted on a periodic basis throughout a County employee's term of employment with the County.

Periodic information security awareness training shall must be provided to all County IT users of County IT resources and should be documented to assist County Department management in determining user employee awareness and participation. County IT users shall must be aware of basic information security requirements and their responsibility to protect all information (personal information, confidential information, and other).

Each County Department shall ensure that its County IT users participate in the countywide information security awareness training program as well as any additional County Department information security awareness training programs. County Departments may develop additional information security awareness training programs based on their specific needs and sensitivity of information.

~~The Chief Information Office (CIO) shall facilitate and coordinate with County departments to establish and maintain a countywide information security awareness training program. This program will be based on County IT security policies to ensure County IT resources (i.e., hardware, software, information, etc.) are not compromised.~~

~~County departments may develop additional information security awareness training programs based on their specific needs and sensitivity of information. Each County department shall ensure its employees/users participate in the countywide as well as any specific departmental information security awareness training programs.~~

Information security awareness training shall be provided to County IT users

employees/users as appropriate to their job function, duties, and responsibilities.

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

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

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

Requests for exceptions to this Board of Supervisors (Board) policy shall must be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO) and shall require approved by the Board. ~~of Supervisors.~~ County Departments requesting exceptions shall ~~should~~ provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall ~~will~~ review such requests, confer with the

requesting County Department, and place the matter on the Board's agenda along with a recommendation for Board action.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007

Reissue Date:

Sunset Review Date: May 8, 2011

Sunset Review Date:

DRAFT



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.112	Secure Disposition of Computing Devices	10/23/07

PURPOSE

To ensure that all information and software on County-owned or leased computing devices are protected from unauthorized disclosure prior to disposition of such computing devices out of County inventory or transfer of such computing devices to other users.

REFERENCE

October 23, 2007, [Board Order No. 22 – Board of Supervisors – Information Technology and Security Policy](#)

Board of Supervisors Policy No. [6.100](#) – Information Technology and Security Policy

[Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources \(Acceptable Use Agreement\), attached thereto](#)

~~Chief Information Officer's Memo "[Countywide Information Technology and Security Policy](#)"~~

Board of Supervisors Policy [3.040](#) – General Records Retention and Protection of Records Containing Personal and Confidential Information

POLICY

[This policy is applicable to all County IT users.](#)

[Each County Department shall comply with the County IT security standards and procedures set forth by the Information Security Steering Committee \(ISSC\) in support of this policy.](#)

Each County Department is responsible for ensuring that all information and software on County-owned or leased computing devices are rendered unreadable and unrecoverable, whether or not removed from such computing devices, prior to disposition of such computing devices out of County inventory, to prevent unauthorized use or disclosure.

Each County Department is responsible for ensuring that all personal and confidential information on County-owned or leased computing devices is rendered unreadable when such computing devices are transferred to other users who are not authorized to access the personal and confidential information.

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

Dispositions of County-owned or leased computing devices out of County inventory include, without limitation, the following:

~~Computing devices include, without limitation, the following:~~

- ~~• Personal computers, such as desktops, laptops, and personal digital assistants (PDA)~~
- ~~• Multiple user and application computers, such as servers~~
- ~~• Portable storage media, such as diskettes, tapes, CDs, zip disks, DVDs, flash memory/drives, and USB drives~~

~~Dispositions of County-owned or leased computing devices out of County inventory include, without limitation, the following:~~

- Computing device sent to salvage
- Computing device destroyed
- Computing device donated to a non-County organization

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "computing devices" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and

Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy.

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

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

There are no exemptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: October 23, 2007

Reissue Date:

Sunset Review Date: October 23, 2011

Sunset Review Date: