



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

WILLIAM T FUJIOKA
Chief Executive Officer

DATE: May 15, 2014
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 – Santos H. Kreimann
 - A) **Board Letter – APPROVAL OF AMENDMENT TO AGREEMENT WITH LANCET TECHNOLOGY, INC.**
DHS/CIO – Mitchell H. Katz and Richard Sanchez or designee(s)
 - B) **Board Letter – COUNTYWIDE CLASSIFICATION ACTIONS TO IMPLEMENT THE FY 2014-15 RECOMMENDED BUDGET**
CEO Class/Comp – Steve Masterson or designee
 - C) **Performance Management Tracking System and Dashboards**
DHR – Lisa Garrett or designee
 - D) **Review of IT Security Policies 6.100 – 6.112**
CIO – Richard Sanchez or designee
2. Public Comment
3. Adjournment

June 3, 2014

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:

**APPROVAL OF AMENDMENT TO AGREEMENT WITH LANCET
TECHNOLOGY, INC.
(ALL DISTRICTS)
(3 VOTES)**

**CIO RECOMMENDATION: APPROVE ()
APPROVE WITH MODIFICATION () DISAPPROVE ()**

SUBJECT

Approval of an Amendment to extend the term of the Trauma and Emergency Medicine Information System Agreement with Lancet Technology for the Department of Health Services', Emergency Medical Services Agency.

IT IS RECOMMENDED THAT THE BOARD:

1. Authorize the Director of Health Services (Director), or his designee, to execute an Amendment to Agreement H-212780, Lancet Technology (Lancet), effective upon execution to extend term of the Trauma and Emergency Medicine Information System (TEMIS) for two years, with three (3) automatic one-year extension terms to June 30, 2019, unless the County gives prior notice to not extend, and to increase the contract sum by \$4,643,840 from \$9,595,518 to \$14,239,358 for the entire term of the Agreement with the increased costs 100 percent funded by trauma center and base hospital fees.
2. Delegate authority to the Director, or his designee, to amend this Agreement to add, delete and/or change certain terms and conditions as required under Federal or State law or regulation, County policy, or by the County's Board of Supervisors, Chief Executive Officer or designee.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTIONS

Approval of the first recommendation will allow the Director, or his designee, to execute an Amendment, substantially similar to Exhibit I, with Lancet to extend the term of the Agreement for two years through June 30, 2016 with automatic one-year extension terms to June 30, 2019 and to increase the contract sum to pay for the extension periods. County has an option to not extend the extension term with 30-day prior notice. The current Agreement expires June 30, 2014 and the services need to continue.

The recommended extension will enable Lancet to continue to maintain the TEMIS with all existing functionality as defined in the current Agreement. TEMIS is an integrated countywide trauma and emergency data management system used by the Department of Health Services (DHS) Emergency Medical Services (EMS) Agency, and 14 Trauma Hospitals, 21 Base Hospitals, and EMS Provider Agencies. The EMS content and format of the existing TEMIS has been designed and customized for all of the agencies to continually access TEMIS records to generate reports necessary for timely data capture, analysis, and sharing of health intelligence data. The current TEMIS databases contain more than 12 million records with more than 850,000 new records added annually.

Under the current Agreement, Lancet consolidated three separate databases (Fire-Rescue, Base, and Trauma) into one central database that now contains a single record for each patient and developed a TEMIS File Transfer Protocol (FTP) for the secure transfer of confidential patient care records. The current TEMIS has evolved into a complex and customized system that allows for timely data capture, analysis, sharing of health intelligence data, enhanced bio-surveillance, and expedited decision-making for casualty management activities.

Lancet has established a history of responding consistently and quickly to the changing needs and demands of the system participants. Lancet personnel have a comprehensive understanding of the Los Angeles County EMS system and have established and maintained an excellent working relationship with the existing TEMIS participants.

Approval of the second recommendation will allow the Director to add, delete and/or change non-substantive terms and conditions in the Agreement.

Implementation of Strategic Plan Goals

The recommended actions support Goal 1, Operational Effectiveness of the County's Strategic Plan.

FISCAL IMPACT/FINANCING

The maximum obligation under this Agreement including the extension period of July 1, 2014 through June 30, 2019 is \$14,239,358, which will be fully offset by base and trauma center hospital fees.

Funding is included in DHS' Fiscal Year (FY) 2014-15 Recommended Budget and will be requested in future years' budgets.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The Board approved the sole source Agreement with Lancet to continue maintenance of the TEMIS for the EMS Agency on June 7, 2001. Subsequent amendments were approved to upgrade system hardware and extend the Agreement term through June 30, 2014. During the extension period, DHS plans to conduct a competitive solicitation for continuation of these services

The recommended Amendment includes all updated Board required provisions. The Agreement may be terminated for convenience by the County upon 30-day prior written notice.

County Counsel has approved Exhibit I as to form and the County's Chief Information Officer recommends approval of this Agreement (Attachment A).

The TEMIS services is not a Proposition A Agreement as the services are highly specialized and cannot currently be provided by County staff, and are therefore not subject to the Living Wage Program (Los Angeles County Code Chapter 2.201).

CONTRACTING PROCESS

The current Agreement with Lancet needs to be amended to allow for sufficient time for DHS to conduct a solicitation for a replacement system for EMS and the other participating agencies.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of the recommendations will ensure that EMS continues to provide uninterrupted critical patient-care needs using the TEMIS for the sharing of health intelligence data.

Respectfully submitted,

Reviewed by:

The Honorable Board of Supervisors
June 3, 2014
Page 4

Mitchell H. Katz, M.D.
Director

Richard Sanchez
Chief Information Officer

MHK:sa

Enclosures (2)

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



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>

WILLIAM T FUJIOKA
Chief Executive Officer

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

June 4, 2014

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:

COUNTYWIDE CLASSIFICATION ACTIONS TO IMPLEMENT THE FISCAL YEAR 2014-2015 RECOMMENDED BUDGET (ALL SUPERVISORIAL DISTRICTS) (3 VOTES)

SUBJECT

This letter and accompanying ordinance will update the County Classification Plan and departmental staffing provisions by adding one (1) new unclassified classification, by deleting one (1) non-represented classification, by changing the salary of two (2) non-represented classifications, and by implementing classification actions countywide in conjunction with the Fiscal Year (FY) 2014-2015 Recommended Budget as recommended by the Chief Executive Office.

IT IS RECOMMENDED THAT THE BOARD:

Approve the accompanying ordinance amending Title 6, Salaries, of the County Code to add one (1) new unclassified classification, to delete one (1) non-represented classification, to change the salary of two (2) non-represented classifications, and to update the departmental provisions to reflect positions allocated, deleted and transferred in the FY 2014-2015 Recommended Budget.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The majority of actions recommended in this letter are budget related, and were approved - in concept - by the Board of Supervisors (Board) as part of the FY 2014-2015 Recommended Budget on April 15, 2014. Since that time, we have been working to gather and analyze the required information to determine and allocate the appropriate

classification and level of new positions. This letter implements these specific changes to the departmental staffing provisions to be effective July 1, 2014.

The Board's approval of this ordinance will fulfill the Charter requirement to provide, by ordinance, for the number of County employees. It will also provide the authority for County departments to fill new positions allocated in the FY 2014-2015 Recommended Budget, delete positions no longer needed, and make other adjustments as necessary. These recommendations are a routine part of the annual budget process.

New Unclassified Classification

In conjunction with a reorganization of the Executive Office, Board of Supervisors, one (1) new unclassified classification is being established in the Executive Office, Board of Supervisors (Attachment A). The Assistant Executive Officer, Board of Supervisors (UC) will report directly to the Executive Officer, Board of Supervisors (UC) and will direct, plan, manage and implement the operational and administrative functions of the Executive Office, including fiscal, budget, and Board of Supervisors' meeting agendas. This new classification will allow for the proper alignment of current and newly assigned divisions within the Executive Office.

Deleted Classification

In conjunction with our continuing goal of reducing classifications, we are recommending the deletion of one (1) non-represented classification (Attachment A). This recommendation is consistent with the County's strategy to reduce the number of obsolete classifications.

Salary Changes

We are recommending a salary range adjustment for two (2) non-represented Management Appraisal and Performance Plan (MAPP) classifications (Attachment A). Specifically, we are recommending a salary range increase for the position of Executive Director, Arts Commission from salary range R12 to R15, to recognize the expanding role of the Arts Commission and the unique knowledge and experience required to perform the complex duties of the position. While there is clearly only one Executive Director, Arts Commission in the County, there are two related classifications in the Plan (classified and unclassified). We are changing the salary of both these classes to R15.

Technical Adjustments and Corrections

In addition to classification actions directly related to the FY 2014-2015 approved budget, other technical and routine adjustments and corrections are being made to the staffing provisions of various County departments to reflect earlier Board-approved budget and classification actions. These adjustments include position adjusting entries from previous classification actions such as classification studies, reorganizations, and midyear allocations.

Implementation of Strategic Plan Goals

Approval of the accompanying ordinance will further the County Strategic Plan, Workforce Excellence and Organization Effectiveness Goals, to improve the quality of the workforce, to achieve departmental operational needs, and to maintain consistency in personnel practices throughout the County.

FISCAL IMPACT/FINANCING

The cost of and financing for the new position recommendations have been included in the FY 2014-2015 Recommended Budget. The projected budgeted annual cost for the salary changes is estimated to total \$36,721. Net County cost is estimated to be \$36,306. Cost increases associated with the compensation changes will be absorbed within the Board's adopted budget for the affected department. No additional funding is required.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The County Charter authorizes the establishment and maintenance of "a classification plan and the classification of all positions." This responsibility is further delineated in Civil Service Rule 5.

The accompanying ordinance implementing amendments to Title 6, Salaries, of the County Code has been approved as to form by County Counsel.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Your approval of these recommendations will enable departments to effect personnel actions associated with the recently approved budget for FY 2014-2015 and various classification studies. Ultimately, this will enhance the quality of services provided to the public and the operational effectiveness of the departments.

The Honorable Board of Supervisors
June 4, 2014
Page 4

Respectfully submitted,

WILLIAM T FUJIOKA
Chief Executive Officer

WTF:JA
SJM:mmg

Attachment

c: Executive Office, Board of Supervisors
County Counsel
Auditor-Controller
Department of Human Resources
Affected Departments

n:\classification\abcd - board letters - working file\fy 14-15 recommended budget\fy 14-15 recommended budget board letter (1).doc

ATTACHMENT A

**UNCLASSIFIED CLASSIFICATION RECOMMENDED
FOR ADDITION TO THE CLASSIFICATION PLAN**

Proposed Savings/Cafeteria Benefit Plan	Item No.	Title	Salary Schedule & Level
Savings/Megaflex	1114	Assistant Executive Officer, Board of Supervisors (UC)	N23 R16

**NON-REPRESENTED CLASSIFICATION
RECOMMENDED FOR DELETION**

Item No.	Title
4725	Chief, Administrative Support Bureau, Mental Health

**NON-REPRESENTED MAPP CLASSIFICATIONS
RECOMMENDED FOR SALARY CHANGE**

Item No.	Title	Current Salary Schedule and Level		Recommended Salary Schedule and Level	
8807	Executive Director, Arts Commission	N23	R12	N23	R15
8808	Executive Director, Arts Commission (UC)	N23	R12	N23	R15

ANALYSIS

This ordinance amends Title 6 - Salaries, of the Los Angeles County Code by:

- Adding and establishing the salary for one (1) unclassified employee classification;
- Deleting one (1) non-represented employee classification;
- Changing the salaries of two (2) non-represented employee classifications; and
- Adding, deleting, and/or changing certain classifications and numbers of ordinance positions in the departments of Agricultural Commissioner/Weights and Measures, Alternate Public Defender, Animal Care and Control, Assessor, Auditor-Controller, Beaches and Harbors, Board of Supervisors, Chief Executive Officer, Chief Information Officer, Child Support Services, Children and Family Services, Community and Senior Services, Consumer Affairs, County Counsel, District Attorney, Fire, Health Services, Human Resources, Internal Services, Medical Examiner-Coroner, Mental Health, Military and Veterans Affairs, Museum of Natural History, Parks and Recreation, Probation, Public Health, Public Library, Public Social Services, Public Works, Regional Planning, Sheriff, and Treasurer and Tax Collector.

JOHN F. KRATTLI
County Counsel

By: _____
RICHARD D. BLOOM
Principal Deputy County Counsel
Labor & Employment Division

RDB:

ORDINANCE NO. _____

An ordinance amending Title 6 - Salaries, of the Los Angeles County Code relating to the salary changes and to the addition, deletion, and changing of certain classifications and number of ordinance positions in various departments as a result of the budget process for FY 2014-2015.

The Board of Supervisors of the County of Los Angeles ordains as follows:

SECTION 1. Section 6.28.050 is hereby amended to add the following class:

ITEM NO.	TITLE	EFFECTIVE DATE	SALARY OR SALARY SCHEDULE AND LEVEL
<u>1114</u>	<u>ASST EXEC OFFICER,BD OF SUP(UC)</u>	_____ *	<u>N23</u> <u>R16</u>

SECTION 2. Section 6.28.050 is hereby amended to delete the following class:

ITEM NO.	TITLE	EFFECTIVE DATE	SALARY OR SALARY SCHEDULE AND LEVEL
4725	CHIEF,ADMIN SUPPORT BUREAU,MH	01/01/2009	NM 103K
		10/01/2013	NM 104G
		10/01/2014	NM 105D
		04/01/2015	NM 106A

SECTION 3. Section 6.28.050 is hereby amended to change only the salary of the following classes:

ITEM NO.	TITLE	EFFECTIVE DATE	SALARY OR SALARY SCHEDULE AND LEVEL		
8807	EXEC DIRECTOR,ARTS COMMISSION	01/01/2009	N23	R12	
		10/01/2013	N23	R12	
		10/01/2014	N23	R12	
		04/01/2015	<u>N23</u>	R12	
			*	<u>N23</u>	<u>R15</u>
		10/01/2014	<u>N23</u>	<u>R15</u>	
		04/01/2015	<u>N23</u>	<u>R15</u>	
8808	EXEC DIRECTOR,ARTS COMMISSION(UC)	01/01/2009	N23	R12	
		10/01/2013	N23	R12	
		10/01/2014	N23	R12	
		04/01/2015	<u>N23</u>	R12	
			*	<u>N23</u>	<u>R15</u>
		10/01/2014	<u>N23</u>	<u>R15</u>	
		04/01/2015	<u>N23</u>	<u>R15</u>	

SECTION 4. Section 6.32.010 (Agricultural Commissioner/Weights and Measures) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0012A	4	AGRICULTURAL INSPECTOR III
0012N	4	AGRICULTURAL INSPECTOR III

SECTION 5. Section 6.32.010 (Agricultural Commissioner/Weights and Measures) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0009A	120 <u>121</u>	AGRIC/WEIGHTS & MEAS INSPECTOR II
0044A	8 <u>10</u>	PEST CONTROL WORKER

SECTION 6. Section 6.33.010 (Alternate Public Defender) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
9259A	4 <u>5</u>	DIVISION CHIEF,PUBLIC DEFENDER
9253A	48 <u>17</u>	HEAD DEPUTY PUBLIC DEFENDER

SECTION 7. Section 6.34.010 (Department of Animal Care and Control) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
2979A	87 <u>89</u>	ANIMAL CONTROL OFFICER I
2980A	68 <u>72</u>	ANIMAL CONTROL OFFICER II
2214A	33 <u>39</u>	INTERMEDIATE TYPIST-CLERK
2219A	4 <u>5</u>	SUPERVISING TYPIST-CLERK

SECTION 8. Section 6.38.010 (Assessor) is hereby amended to delete the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1000A	4	ADMIN SERVICES MANAGER III,ASSESSOR

SECTION 9. Section 6.38.010 (Assessor) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>1004A</u>	<u>1</u>	<u>ADMINISTRATIVE SERVICES MANAGER III</u>

SECTION 10. Section 6.40.010 (Auditor-Controller) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0646A	3 <u>4</u>	ACCOUNTANT I
0677A	35 <u>38</u>	INTERMEDIATE ACCOUNTANT-AUDITOR
1848A	2 <u>3</u>	MANAGEMENT ANALYST
0712A	20 <u>21</u>	PROGRAM SPECIALIST I,AUDITOR-CONT
0650A	49 <u>21</u>	SENIOR ACCOUNTANT,AUDITOR-CONT
0679A	44 <u>43</u>	SENIOR ACCOUNTANT-AUDITOR
1366A	3 <u>2</u>	TAX SERVICES CLERK I

1367A 48 16 TAX SERVICES CLERK II

SECTION 11. Section 6.42.010 (Department of Beaches and Harbors) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>0577A</u>	<u>1</u>	<u>ACCOUNT CLERK I</u>

SECTION 12. Section 6.42.010 (Department of Beaches and Harbors) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
8861A	3 <u>4</u>	CONTRACT MONITOR,RECREATIONAL SVCS
1140A	2 <u>3</u>	SENIOR CLERK

SECTION 13. Section 6.44.010 (Department of the Board of Supervisors) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1101A	2 <u>3</u>	DEP EXECUTIVE OFFICER,BD OF SUP(UC)
1100A	38 <u>39</u>	SENIOR BOARD SPECIALIST

SECTION 14. Section 6.50.010 (Department of the Chief Executive Officer) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0819A	29 <u>30</u>	CHIEF PROGRAM SPECIALIST,CEO
8697A	6 <u>7</u>	CLINICAL PSYCHOLOGIST II
0817A	60 <u>62</u>	PROGRAM SPECIALIST III,CEO
0818A	36 <u>37</u>	PROGRAM SPECIALIST IV,CEO

SECTION 15. Section 6.51.010 (Chief Information Officer) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>0889A</u>	<u>1</u>	<u>ADMINISTRATIVE ASSISTANT III</u>
<u>2593A</u>	<u>1</u>	<u>SENIOR INFORMATION SYSTEMS ANALYST</u>

SECTION 16. Section 6.52.010 (Department of Medical Examiner-Coroner) is hereby amended to delete the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
4009L	4	DIRECTOR,DEPARTMENT OF CORONER

SECTION 17. Section 6.52.010 (Department of Medical Examiner-Coroner) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>1848A</u>	<u>1</u>	<u>MANAGEMENT ANALYST</u>
<u>3036A</u>	<u>1</u>	<u>SAFETY OFFICER</u>

SECTION 18. Section 6.52.010 (Department of Medical Examiner-Coroner) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1637A	44 <u>42</u>	CORONER INVESTIGATOR
2214A	9 <u>10</u>	INTERMEDIATE TYPIST-CLERK
4336A	43 <u>14</u>	SENIOR CRIMINALIST

SECTION 19. Section 6.53.010 (Department of Children and Family Services) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>2565A</u>	<u>1</u>	<u>INFORMATION TECHNOLOGY MANAGER I</u>
<u>2594A</u>	<u>1</u>	<u>PRINCIPAL INFO SYSTEMS ANALYST</u>
<u>5237A</u>	<u>1</u>	<u>PROGRAM SPECIALIST,PUB HLTH NURSING</u>
<u>3034A</u>	<u>4</u>	<u>SAFETY INSPECTOR</u>

SECTION 20. Section 6.53.010 (Department of Children and Family Services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0888A	49 <u>20</u>	ADMINISTRATIVE ASSISTANT II
1002A	56 <u>58</u>	ADMINISTRATIVE SERVICES MANAGER I
2521A	3 <u>5</u>	APPLICATION DEVELOPER II
9073A	3342 <u>3448</u>	CHILDREN'S SOCIAL WORKER III
9177A	2 <u>4</u>	ELIGIBILITY WORKER III
8995A	68 <u>89</u>	HUMAN SERVICES AIDE
2591A	40 <u>12</u>	INFORMATION SYSTEMS ANALYST II
2214A	789 <u>811</u>	INTERMEDIATE TYPIST-CLERK
1848A	7 <u>12</u>	MANAGEMENT ANALYST
2110A	4 <u>2</u>	MANAGEMENT SECRETARY IV
2526A	7 <u>10</u>	PRINCIPAL APPLICATION DEVELOPER
2096A	447 <u>120</u>	SECRETARY III
2525A	44 <u>15</u>	SENIOR APPLICATION DEVELOPER
9109A	4 <u>2</u>	SR DEP DIR,CHILD & FAMILY SERVICES(UC)
2593A	5 <u>9</u>	SENIOR INFORMATION SYSTEMS ANALYST
2102A	34 <u>35</u>	SENIOR SECRETARY III

SECTION 21. Section 6.55.010 (Child Support Services Department) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0889A	6 <u>5</u>	ADMINISTRATIVE ASSISTANT III
1003A	4 <u>5</u>	ADMINISTRATIVE SERVICES MANAGER II
9008A	3 <u>2</u>	APPEALS HEARING SPECIALIST
9285A	40 <u>34</u>	ATTORNEY II,CHILD SUPPORT SERVS
9286A	34 <u>37</u>	ATTORNEY III,CHILD SUPPORT SERVS
1614A	794 <u>756</u>	CHILD SUPPORT OFFICER II
1615A	156 <u>151</u>	CHILD SUPPORT OFFICER III
1618A	34 <u>32</u>	HEAD CHILD SUPPORT OFFICER
2161A	26 <u>23</u>	LEGAL OFFICE SUPPORT ASSISTANT II
2109A	4 <u>3</u>	MANAGEMENT SECRETARY III
2593A	2 <u>1</u>	SENIOR INFORMATION SYSTEMS ANALYST

SECTION 22. Section 6.58.010 (Department of Community and Senior Services) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>8103F</u>	<u>5</u>	<u>COMMUNITY WORKER</u>

SECTION 23. Section 6.58.010 (Department of Community and Senior Services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS		TITLE
8021A	2	<u>3</u>	HUMAN SERVICES ADMINISTRATOR I
9051A	55	<u>59</u>	SOCIAL WORKER
8258F	6	<u>4</u>	STUDENT PROFESSIONAL WORKER II

SECTION 24. Section 6.60.010 (Department of Consumer Affairs) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS		TITLE
<u>1668N</u>	<u>2</u>		<u>CONSUMER AFFAIRS SUPERVISOR</u>
<u>1848A</u>	<u>1</u>		<u>MANAGEMENT ANALYST</u>

SECTION 25. Section 6.60.010 (Department of Consumer Affairs) is hereby amended to change the number of ordinance positions for the following class:

ITEM NO.	NO. OF ORDINANCE POSITIONS		TITLE
1664N	7	<u>14</u>	CONSUMER AFFAIRS REPRESENTATIVE III

SECTION 26. Section 6.64.010 (County Counsel) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1120A	4	EXECUTIVE ASSISTANT
2219A	4	SUPERVISING TYPIST-CLERK

SECTION 27. Section 6.64.010 (County Counsel) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
9206A	90 <u>93</u>	DEPUTY COUNTY COUNSEL
2214A	43 <u>12</u>	INTERMEDIATE TYPIST-CLERK
2915A	2 <u>1</u>	INVESTIGATOR II
2111A	5 <u>6</u>	MANAGEMENT SECRETARY V
9217A	4 <u>5</u>	SENIOR ASSISTANT COUNTY COUNSEL(UC)
9207A	473 <u>176</u>	SENIOR DEPUTY COUNTY COUNSEL
9243A	2 <u>1</u>	SENIOR LAW CLERK

SECTION 28. Section 6.70.010 (District Attorney) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS		TITLE
9273N	36	<u>37</u>	DEPUTY DISTRICT ATTORNEY III
2890N	24	<u>22</u>	SENIOR INVESTIGATOR,DA

SECTION 29. Section 6.76.010 (Fire Department – Executive) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS		TITLE
<u>1120F</u>	<u>1</u>		<u>EXECUTIVE ASSISTANT</u>

SECTION 30. Section 6.76.010 (Fire Department – Executive) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS		TITLE
2214A	40	<u>9</u>	INTERMEDIATE TYPIST-CLERK
1598A	4	<u>2</u>	PUBLIC INFORMATION ASSISTANT

SECTION 31. Section 6.76.011 (Fire Department – Administrative) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>1061A</u>	<u>1</u>	<u>CHIEF, FINANCIAL MANAGEMENT, FIRE</u>

SECTION 32. Section 6.76.011 (Fire Department – Administrative) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1002A	44 <u>12</u>	ADMINISTRATIVE SERVICES MANAGER I
1003A	3 <u>4</u>	ADMINISTRATIVE SERVICES MANAGER II
0748A	4 <u>2</u>	FINANCIAL SPECIALIST II
2214A	44 <u>12</u>	INTERMEDIATE TYPIST-CLERK
2344A	8 <u>12</u>	PROCUREMENT ASSISTANT I
2346A	6 <u>7</u>	PROCUREMENT ASSISTANT II
1843A	3 <u>4</u>	SENIOR DEPARTMENTAL PERSONNEL ASST
1849A	6 <u>7</u>	SENIOR DEPARTMENTAL PERSONNEL TECH

SECTION 33. Section 6.76.014 (Fire Department – Operations) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0217A	42 <u>15</u>	ASSISTANT FIRE CHIEF
0208A	73 <u>86</u>	BATTALION CHIEF(56 HOURS)
0205A	632 <u>684</u>	FIRE CAPTAIN(56 HOURS)
0201A	712 <u>753</u>	FIRE FIGHTER SPECIALIST(56 HOURS)
2102A	40 <u>11</u>	SENIOR SECRETARY III

SECTION 34. Section 6.76.016 (Fire Department – Special services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
2521A	5 <u>6</u>	APPLICATION DEVELOPER II
4125A	4 <u>9</u>	FACILITIES PROJECT MANAGER I
2432A	8 <u>4</u>	FIRE DISPATCHER I
2433A	80 <u>84</u>	FIRE DISPATCHER II
2525A	2 <u>3</u>	SENIOR APPLICATION DEVELOPER

SECTION 35. Section 6.76.017 (Fire Department – Leadership and Professional Standards) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>1843A</u>	<u>1</u>	<u>SENIOR DEPARTMENTAL PERSONNEL ASST</u>

SECTION 36. Section 6.76.017 (Fire Department – Leadership and Professional Standards) is hereby amended to change the number of ordinance positions for the following class:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1881A	40 <u>12</u>	DEPARTMENTAL CIVIL SERVICE REP

SECTION 37. Section 6.77.010 (Department of Public Health – Public health services) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0886F	4	ADMINISTRATIVE AID
2559A	4	NETWORK SYSTEMS ADMINISTRATOR II
9194N	4	SUPVG PATIENT FIN SERVICE WORKER I

SECTION 38. Section 6.77.010 (Department of Public Health – Public health services) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>0577A</u>	<u>2</u>	<u>ACCOUNT CLERK I</u>
<u>1907A</u>	<u>1</u>	<u>DEPARTMENTAL EMPLOYEE RELATIONS REP</u>
<u>4729A</u>	<u>1</u>	<u>HEALTH PROGRAM ANALYST II</u>
<u>0904A</u>	<u>1</u>	<u>MANAGEMENT ASSISTANT</u>
<u>1515A</u>	<u>1</u>	<u>SENIOR DISASTER SERVICES ANALYST</u>
<u>5456A</u>	<u>1</u>	<u>SENIOR PHYSICIAN</u>

SECTION 39. Section 6.77.010 (Department of Public Health – Public health services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0647A	4 <u>6</u>	ACCOUNTANT II
0642A	5 <u>12</u>	ACCOUNTING TECHNICIAN I
5233A	4 <u>5</u>	ASSISTANT PROGRAM SPECIALIST,PHN
4595A	44 <u>13</u>	ASSISTANT STAFF ANALYST,HLTH SERVS
8103A	38 <u>37</u>	COMMUNITY WORKER

8103N	52	<u>51</u>	COMMUNITY WORKER
0672N	7	<u>8</u>	HEALTH CARE FINANCIAL ANALYST
4846A	6	<u>7</u>	HEALTH EDUCATION ASSISTANT
4727A	9	<u>8</u>	HEALTH PROGRAM ANALYST I
4729N	2	<u>3</u>	HEALTH PROGRAM ANALYST II
2591A	7	<u>9</u>	INFORMATION SYSTEMS ANALYST II
2591N	13	<u>12</u>	INFORMATION SYSTEMS ANALYST II
2565A	2	<u>3</u>	INFORMATION TECHNOLOGY MANAGER I
2214N	36	<u>37</u>	INTERMEDIATE TYPIST-CLERK
4899A	4	<u>2</u>	MEDICAL TECHNOLOGIST,DATA SYSTEMS
2559N	-4	<u>5</u>	NETWORK SYSTEMS ADMINISTRATOR II
2594A	7	<u>9</u>	PRINCIPAL INFO SYSTEMS ANALYST
2594N	4	<u>2</u>	PRINCIPAL INFO SYSTEMS ANALYST
5000A	13	<u>14</u>	PUBLIC HEALTH MICROBIOLOGIST II
3033A	4	<u>2</u>	SAFETY ASSISTANT
3034A	4	<u>2</u>	SAFETY INSPECTOR
1140A	3	<u>2</u>	SENIOR CLERK
2593A	10	<u>11</u>	SENIOR INFORMATION SYSTEMS ANALYST
2547A	11	<u>12</u>	SENIOR IT TECHNICAL SUPPORT ANALYST
2560A	6	<u>5</u>	SR NETWORK SYSTEMS ADMINISTRATOR
2560N	-4	<u>5</u>	SR NETWORK SYSTEMS ADMINISTRATOR
4594A	11	<u>12</u>	SENIOR STAFF ANALYST,HEALTH

4593A	24	<u>26</u>	STAFF ANALYST,HEALTH
4593N	35	<u>34</u>	STAFF ANALYST,HEALTH
0907A	-4	<u>5</u>	STAFF ASSISTANT I
0913N	14	<u>15</u>	STAFF ASSISTANT II
8243F	73	<u>72</u>	STUDENT PROFESSIONAL WORKER I
2329A	-4	<u>5</u>	WAREHOUSE WORKER AID

SECTION 40. Section 6.77.020 (Department of Public Health – Substance abuse prevention and control) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>8697N</u>	<u>1</u>	<u>CLINICAL PSYCHOLOGIST II</u>
<u>2584N</u>	<u>2</u>	<u>INFORMATION TECHNOLOGY AIDE</u>
<u>5476N</u>	<u>1</u>	<u>PHYSICIAN SPECIALIST(NON MEGAFLEX)</u>
<u>5134N</u>	<u>5</u>	<u>REGISTERED NURSE II</u>
<u>5125N</u>	<u>1</u>	<u>UTILIZATION REVIEW NURSE SUPVR I</u>

SECTION 41. Section 6.77.025 (Department of Public Health – Children’s medical services) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>9014N</u>	<u>1</u>	<u>CLINICAL SOCIAL WORK SUPERVISOR I</u>

SECTION 42. Section 6.78.010 (Department of Health Services – Administration) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
4848A	4	HEALTH EDUCATOR
1602A	4	PUBLIC INFORMATION REPRESENTATIVE
1861A	4	STAFF DEVELOPMENT SPECIALIST

SECTION 43. Section 6.78.010 (Department of Health Services – Administration) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>5121A</u>	<u>20</u>	<u>NURSE PRACTITIONER</u>
<u>5288A</u>	<u>1</u>	<u>NURSING DIRECTOR, EDUCATION</u>
<u>8062A</u>	<u>1</u>	<u>SR COMMUNITY LIAISON REPRESENTATIVE</u>
<u>8105A</u>	<u>25</u>	<u>SENIOR COMMUNITY WORKER</u>

SECTION 44. Section 6.78.010 (Department of Health Services – Administration) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0578A	9 <u>8</u>	ACCOUNT CLERK II
4595A	24 <u>19</u>	ASSISTANT STAFF ANALYST, HLTH SERVS
5457A	2 <u>3</u>	CHIEF PHYSICIAN I
4614A	24 <u>19</u>	CONTRACT PROGRAM AUDITOR
4614N	3 <u>2</u>	CONTRACT PROGRAM AUDITOR
2591A	23 <u>22</u>	INFORMATION SYSTEMS ANALYST II
2214A	77 <u>75</u>	INTERMEDIATE TYPIST-CLERK

2214N	3	<u>2</u>	INTERMEDIATE TYPIST-CLERK
5214A	24	<u>22</u>	NURSING INSTRUCTOR
5134A	9	<u>8</u>	REGISTERED NURSE II
2096A	7	<u>5</u>	SECRETARY III
2096N	2	<u>1</u>	SECRETARY III
1140A	34	<u>33</u>	SENIOR CLERK
5216A	45	<u>18</u>	SENIOR NURSING INSTRUCTOR
2101A	47	<u>16</u>	SENIOR SECRETARY II
2102A	40	<u>9</u>	SENIOR SECRETARY III
4593A	74	<u>73</u>	STAFF ANALYST,HEALTH
8243F	46	<u>15</u>	STUDENT PROFESSIONAL WORKER I

SECTION 45. Section 6.78.030 (Department of Health Services – Office of managed care) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>1007A</u>	<u>1</u>	<u>ADMINISTRATIVE SERVICES DIV MGR</u>
<u>0753A</u>	<u>1</u>	<u>FISCAL OFFICER II</u>
<u>1773A</u>	<u>1</u>	<u>SENIOR MARKETING ANALYST</u>
<u>1861A</u>	<u>1</u>	<u>STAFF DEVELOPMENT SPECIALIST</u>

SECTION 46. Section 6.78.030 (Department of Health Services – Office of managed care) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0643A	2 <u>3</u>	ACCOUNTING TECHNICIAN II
4595A	5 <u>7</u>	ASSISTANT STAFF ANALYST,HLTH SERVS
5087A	4 <u>12</u>	CLINIC NURSING ATTENDANT I
4614A	3 <u>8</u>	CONTRACT PROGRAM AUDITOR
4848A	2 <u>3</u>	HEALTH EDUCATOR
1138A	13 <u>17</u>	INTERMEDIATE CLERK
1176A	3 <u>4</u>	INTERMEDIATE SUPERVISNG CLERK
2214A	2 <u>3</u>	INTERMEDIATE TYPIST-CLERK
9002A	4 <u>2</u>	MEDICAL CASE WORKER II
9192A	3 <u>15</u>	PATIENT RESOURCES WORKER
5134A	25 <u>27</u>	REGISTERED NURSE II
5135A	6 <u>7</u>	REGISTERED NURSE III
2096A	4 <u>5</u>	SECRETARY III
1140A	2 <u>3</u>	SENIOR CLERK
2216A	30 <u>31</u>	SENIOR TYPIST-CLERK
4593A	13 <u>21</u>	STAFF ANALYST,HEALTH
0907A	11 <u>12</u>	STAFF ASSISTANT I

SECTION 47. Section 6.78.035 (Department of Health Services – Juvenile court health services) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
4976A	4	LABORATORY ASSISTANT
5216A	4	SENIOR NURSING INSTRUCTOR

SECTION 48. Section 6.78.035 (Department of Health Services – Juvenile court health services) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>5701A</u>	<u>1</u>	<u>HLTH FACILITIES CONSULTANT,NURSING</u>

SECTION 49. Section 6.78.035 (Department of Health Services – Juvenile court health services) is hereby amended to change the number of ordinance positions for the following class:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
2219A	3 <u>2</u>	SUPERVISING TYPIST-CLERK

SECTION 50. Section 6.78.055 (Department of Health Services – MetroCare Network) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0578N	1	ACCOUNT CLERK II
5088N	1	CLINIC NURSING ATTENDANT II
7521A	1	MILLWRIGHT
1281A	1	MORTUARY AID
1598A	1	PUBLIC INFORMATION ASSISTANT
5567A	1	PULMONARY PHYSIOLOGY TECHNICIAN I
2216N	1	SENIOR TYPIST-CLERK
0922A	1	STAFF ASSISTANT, NURSING

SECTION 51. Section 6.78.055 (Department of Health Services – MetroCare Network) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>5096A</u>	<u>30</u>	<u>UNIT SUPPORT ASSISTANT</u>
<u>2681A</u>	<u>1</u>	<u>VOLUNTEER PROGRAMS COORDINATOR I</u>

SECTION 52. Section 6.78.055 (Department of Health Services – MetroCare Network) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
5556A	4 <u>3</u>	CARDIOVASCULAR TECHNICIAN
5083A	42 <u>41</u>	CENTRAL SERVICES TECHNICIAN II
5092A	47 <u>68</u>	CERTIFIED MEDICAL ASSISTANT
5090A	51 <u>128</u>	CLINIC LICENSED VOCATIONAL NURSE I
5087A	39 <u>52</u>	CLINIC NURSING ATTENDANT I
5088A	81 <u>73</u>	CLINIC NURSING ATTENDANT II
5604A	2 <u>1</u>	CLINICAL PERFUSION TECHNICIAN
5513A	21 <u>22</u>	CLINICAL PHARMACIST
0927A	3 <u>2</u>	CREDENTIALING SPECIALIST
5794A	46 <u>21</u>	DIAGNOSTIC ULTRASOUND TECHNICIAN
5794F	2 <u>1</u>	DIAGNOSTIC ULTRASOUND TECHNICIAN
0672A	42 <u>10</u>	HEALTH CARE FINANCIAL ANALYST
1153A	3 <u>4</u>	HEALTHCARE INTERPRETER
6346A	2 <u>1</u>	HELPER,CARPENTRY
1138A	222 <u>290</u>	INTERMEDIATE CLERK
2214A	294 <u>278</u>	INTERMEDIATE TYPIST-CLERK
5104A	417 <u>82</u>	LICENSED VOCATIONAL NURSE I

5105A	53	<u>40</u>	LICENSED VOCATIONAL NURSE II
5106A	40	<u>9</u>	LICENSED VOCATIONAL NURSE III
6531A	40	<u>9</u>	MEDICAL ELECTRONICS TECHNICIAN
2135A	46	<u>15</u>	MEDICAL SECRETARY
2180A	42	<u>11</u>	MEDICAL STENOGRAPHER
2209A	31	<u>29</u>	MEDICAL TRANSCRIBER TYPIST
5172A	25	<u>24</u>	NURSE ANESTHETIST II
5286A	44	<u>41</u>	NURSE MANAGER
5359A	40	<u>9</u>	NURSE-MIDWIFE
5121F	6	<u>7</u>	NURSE PRACTITIONER
5098A	28	<u>128</u>	NURSING ATTENDANT I
5100A	130	<u>146</u>	NURSING ATTENDANT II
5101A	59	<u>56</u>	NURSING ATTENDANT III
5595A	9	<u>8</u>	ORTHOPEDIC TECHNICIAN
6973A	47	<u>16</u>	PAINTER
9193A	58	<u>59</u>	PATIENT FINANCIAL SERVS WORKER
9192A	483	<u>186</u>	PATIENT RESOURCES WORKER
5411M	48	<u>49</u>	PHYSICIAN,POST GRADUATE(5TH YEAR)
5411M	39	<u>40</u>	PHYSICIAN,POST GRADUATE(6TH YEAR)
2347A	2	<u>1</u>	PROCUREMENT ASSISTANT III
8162A	24	<u>9</u>	PSYCHIATRIC TECHNICIAN II
5568A	2	<u>1</u>	PULMONARY PHYSIOLOGY TECHNICIAN II

5798A	72	<u>84</u>	RADIOLOGIC TECHNOLOGIST
5798F	2	<u>1</u>	RADIOLOGIC TECHNOLOGIST
5133A	505	<u>579</u>	REGISTERED NURSE I
5134A	450	<u>570</u>	REGISTERED NURSE II
5135A	440	<u>138</u>	REGISTERED NURSE III
5261F	440	<u>380</u>	RELIEF NURSE
2096A	9	<u>8</u>	SECRETARY III
1140A	35	<u>34</u>	SENIOR CLERK
2183A	44	<u>10</u>	SENIOR MEDICAL STENOGRAPHER
5589F	8	<u>7</u>	SR RESPIRATORY CARE PRACTITIONER
2101A	2	<u>1</u>	SENIOR SECRETARY II
2216A	54	<u>49</u>	SENIOR TYPIST-CLERK
5329A	35	<u>34</u>	SUPERVISING CLINIC NURSE I
5338A	49	<u>48</u>	SUPERVISING STAFF NURSE I
2219A	42	<u>11</u>	SUPERVISING TYPIST-CLERK
5111A	43	<u>46</u>	SURGICAL TECHNICIAN
5613A	3	<u>1</u>	UROLOGY TECHNICIAN I

SECTION 53. Section 6.78.060 (Department of Health Services – LAC+USC healthcare network) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
8103F	1	COMMUNITY WORKER
6051A	1	HEAVY TRUCK DRIVER
6349O	1	HELPER, ELECTRICAL
7433A	1	POWER EQUIPMENT TECHNICIAN
7662O	2	SHEET METAL WORKER
1352F	1	STATISTICAL CLERK
5599A	1	SUPERVISING ORTHOPEDIC TECHNICIAN

SECTION 54. Section 6.78.060 (Department of Health Services – LAC+USC healthcare network) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0643A	8 <u>6</u>	ACCOUNTING TECHNICIAN II
5545A	47 <u>16</u>	CARDIAC ELECTRODIAGNOSTIC TECH I
5547A	45 <u>14</u>	CARDIAC ELECTRODIAGNOSTIC TECH III
1253A	9 <u>8</u>	CASHIER

5077A	8	<u>7</u>	CENTRAL SERVICE SUPERVISOR I
5092A	43	<u>73</u>	CERTIFIED MEDICAL ASSISTANT
5090A	55	<u>186</u>	CLINIC LICENSED VOCATIONAL NURSE I
5087A	21	<u>58</u>	CLINIC NURSING ATTENDANT I
5088A	46	<u>17</u>	CLINIC NURSING ATTENDANT II
4895A	155	<u>154</u>	CLINICAL LABORATORY SCIENTIST I
5513A	33	<u>32</u>	CLINICAL PHARMACIST
0927A	5	<u>4</u>	CREDENTIALING SPECIALIST
2657A	2	<u>1</u>	DATA CONTROL CLERK
4745A	4	<u>8</u>	DENTAL ASSISTANT
4749A	2	<u>1</u>	DENTAL LAB RADIOLOGIC TECHNICIAN
6346A	4	<u>3</u>	HELPER,CARPENTRY
6766A	20	<u>19</u>	INSTITUTIONAL LABORER
1138A	331	<u>364</u>	INTERMEDIATE CLERK
2172A	4	<u>3</u>	INTERMEDIATE STENOGRAPHER
1176A	6	<u>5</u>	INTERMEDIATE SUPERVISING CLERK
2214A	275	<u>273</u>	INTERMEDIATE TYPIST-CLERK
1167A	41	<u>10</u>	INVOICE CLERK
4976A	63	<u>62</u>	LABORATORY ASSISTANT
6832A	46	<u>14</u>	LAUNDRY WORKER
5104A	73	<u>49</u>	LICENSED VOCATIONAL NURSE I
5105A	70	<u>46</u>	LICENSED VOCATIONAL NURSE II

5106A	6	<u>5</u>	LICENSED VOCATIONAL NURSE III
7081A	3	<u>2</u>	MEDICAL PHOTOGRAPHER
2135A	6	<u>4</u>	MEDICAL SECRETARY
2180A	40	<u>9</u>	MEDICAL STENOGRAPHER
5121A	424	<u>125</u>	NURSE PRACTITIONER
5098A	364	<u>351</u>	NURSING ATTENDANT I
5100A	255	<u>240</u>	NURSING ATTENDANT II
5101A	406	<u>93</u>	NURSING ATTENDANT III
1611A	2	<u>1</u>	PATIENT RELATIONS SPECIALIST
9192A	498	<u>195</u>	PATIENT RESOURCES WORKER
5568A	24	<u>20</u>	PULMONARY PHYSIOLOGY TECHNICIAN II
5569A	7	<u>6</u>	PULMONARY PHYSIOLOGY TECHNICIAN III
5566A	6	<u>5</u>	PULMONARY PHYSIOLOGY TECH SUPVR I
5133A	952	<u>1142</u>	REGISTERED NURSE I
5133F	404	<u>102</u>	REGISTERED NURSE I
5134A	827	<u>967</u>	REGISTERED NURSE II
5135A	488	<u>272</u>	REGISTERED NURSE III
2096A	22	<u>21</u>	SECRETARY III
2097A	9	<u>8</u>	SECRETARY IV
1140A	99	<u>98</u>	SENIOR CLERK
2183A	40	<u>9</u>	SENIOR MEDICAL STENOGRAPHER
5216A	43	<u>12</u>	SENIOR NURSING INSTRUCTOR

2216A	72	<u>71</u>	SENIOR TYPIST-CLERK
0907A	44	<u>12</u>	STAFF ASSISTANT I
7760A	-4	<u>3</u>	STEAM FITTER & REFRIG WKG SUPVR
8242F	34	<u>32</u>	STUDENT WORKER
4903A	49	<u>18</u>	SUPVG CLINICAL LAB SCIENTIST I
5338A	422	<u>119</u>	SUPERVISING STAFF NURSE I
5111A	52	<u>53</u>	SURGICAL TECHNICIAN
6065A	6	<u>2</u>	TRAM OPERATOR
5096A	3	<u>52</u>	UNIT SUPPORT ASSISTANT

SECTION 55. Section 6.78.065 (Department of Health Services – Rancho Los Amigos) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
5094A	4	CLINIC LICENSED VOCATIONAL NURSE II
5088A	2	CLINIC NURSING ATTENDANT II
6049A	4	MEDIUM TRUCK DRIVER
5568A	4	PULMONARY PHYSIOLOGY TECHNICIAN II
2482F	4	STUDENT PROF WORKER, INFO TECH
5599A	4	SUPERVISING ORTHOPEDIC TECHNICIAN
5614A	4	UROLOGY TECHNICIAN II

SECTION 56. Section 6.78.065 (Department of Health Services – Rancho Los Amigos) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>5092A</u>	<u>18</u>	<u>CERTIFIED MEDICAL ASSISTANT</u>

SECTION 57. Section 6.78.065 (Department of Health Services – Rancho Los Amigos) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0578A	6 <u>3</u>	ACCOUNT CLERK II
5090A	4 <u>12</u>	CLINIC LICENSED VOCATIONAL NURSE I
5087A	5 <u>4</u>	CLINIC NURSING ATTENDANT I
5208A	6 <u>5</u>	CLINICAL INSTRUCTOR, RN
5299A	3 <u>2</u>	CLINICAL NURSING DIRECTOR II
0672A	7 <u>8</u>	HEALTH CARE FINANCIAL ANALYST
2546A	6 <u>9</u>	IT TECHNICAL SUPPORT ANALYST II
1138A	49 <u>65</u>	INTERMEDIATE CLERK
6834A	6 <u>5</u>	INTERMEDIATE LAUNDRY WORKER
2214A	58 <u>56</u>	INTERMEDIATE TYPIST-CLERK

5104A	69	<u>36</u>	LICENSED VOCATIONAL NURSE I
5098A	99	<u>154</u>	NURSING ATTENDANT I
5100A	37	<u>42</u>	NURSING ATTENDANT II
5595A	4	<u>2</u>	ORTHOPEDIC TECHNICIAN
5133A	469	<u>179</u>	REGISTERED NURSE I
5134A	455	<u>162</u>	REGISTERED NURSE II
5135A	36	<u>41</u>	REGISTERED NURSE III
5588A	42	<u>11</u>	RESPIRATORY CARE PRACTITIONER
2096A	2	<u>1</u>	SECRETARY III
1174A	7	<u>6</u>	SUPERVISING CLERK
5338A	29	<u>26</u>	SUPERVISING STAFF NURSE I
5111A	7	<u>6</u>	SURGICAL TECHNICIAN
5096A	43	<u>20</u>	UNIT SUPPORT ASSISTANT

SECTION 58. Section 6.78.070 (Department of Health Services – ValleyCare Network) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1153A	4	HEALTHCARE INTERPRETER
2172A	4	INTERMEDIATE STENOGRAPHER
5608A	4	OPHTHALMOLOGY TECHNICIAN
5595A	2	ORTHOPEDIC TECHNICIAN

5514F	4	RADIOPHARMACIST
5133N	4	REGISTERED NURSE I

SECTION 59. Section 6.78.070 (Department of Health Services – ValleyCare Network) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>5465A</u>	<u>1</u>	<u>CHIEF PHYSICIAN I(NO SPECIALTY)</u>
<u>9034A</u>	<u>2</u>	<u>PSYCHIATRIC SOCIAL WORKER I</u>
<u>5096A</u>	<u>18</u>	<u>UNIT SUPPORT ASSISTANT</u>

SECTION 60. Section 6.78.070 (Department of Health Services – ValleyCare Network) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0577A	44 <u>8</u>	ACCOUNT CLERK I
0578A	40 <u>6</u>	ACCOUNT CLERK II
8044A	-4 <u>3</u>	ASSISTANT HOSPITAL ADMINISTRATOR IV
5545A	4 <u>2</u>	CARDIAC ELECTRODIAGNOSTIC TECH I
5092A	-45 <u>62</u>	CERTIFIED MEDICAL ASSISTANT

5090A	58	<u>105</u>	CLINIC LICENSED VOCATIONAL NURSE I
5087A	34	<u>44</u>	CLINIC NURSING ATTENDANT I
5088A	53	<u>45</u>	CLINIC NURSING ATTENDANT II
5468J	8	<u>7</u>	CLINIC PHYSICIAN,MD(PER SESSION)
6354A	2	<u>1</u>	HELPER,PAINTING
1138A	126	<u>136</u>	INTERMEDIATE CLERK
2214A	300	<u>290</u>	INTERMEDIATE TYPIST-CLERK
5104A	40	<u>28</u>	LICENSED VOCATIONAL NURSE I
5105A	28	<u>23</u>	LICENSED VOCATIONAL NURSE II
9002A	46	<u>18</u>	MEDICAL CASE WORKER II
5121A	56	<u>65</u>	NURSE PRACTITIONER
5121N	2	<u>1</u>	NURSE PRACTITIONER
5121F	3	<u>2</u>	NURSE PRACTITIONER
5098A	45	<u>53</u>	NURSING ATTENDANT I
5100A	456	<u>124</u>	NURSING ATTENDANT II
9193A	61	<u>58</u>	PATIENT FINANCIAL SERVS WORKER
5421F	9	<u>8</u>	PHYSICIAN,MD,OT
8162A	45	<u>5</u>	PSYCHIATRIC TECHNICIAN II
5133A	382	<u>403</u>	REGISTERED NURSE I
5134A	318	<u>354</u>	REGISTERED NURSE II
5135A	77	<u>86</u>	REGISTERED NURSE III
5261F	487	<u>201</u>	RELIEF NURSE

2216A	35	<u>34</u>	SENIOR TYPIST-CLERK
8242F	7	<u>6</u>	STUDENT WORKER
5338A	49	<u>50</u>	SUPERVISING STAFF NURSE I
5111A	46	<u>14</u>	SURGICAL TECHNICIAN

SECTION 61. Section 6.80.010 (Department of Human Resources) is hereby amended to delete the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
4044A	4	ADMINISTRATIVE DEPUTY II

SECTION 62. Section 6.80.010 (Department of Human Resources) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>1045A</u>	<u>1</u>	<u>ADMINISTRATIVE DEPUTY II(UC)</u>

SECTION 63. Section 6.80.010 (Department of Human Resources) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1913A	64	<u>62</u> HUMAN RESOURCES ANALYST IV
1913F	6	<u>5</u> HUMAN RESOURCES ANALYST IV
0913A	8	<u>10</u> STAFF ASSISTANT II

SECTION 64. Section 6.81.010 (Internal Services Department) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>6819A</u>	<u>4</u>	<u>BUILDING COMPLEX MANAGER II</u>
<u>6805A</u>	<u>1</u>	<u>MANAGER,AREA CUSTODIAL OPERATIONS</u>

SECTION 65. Section 6.81.010 (Internal Services Department) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0888A	8 <u>10</u>	ADMINISTRATIVE ASSISTANT II
1003A	34 <u>34</u>	ADMINISTRATIVE SERVICES MANAGER II
2535A	49 <u>18</u>	INFO SYSTEMS SUPPORT ANALYST II
2548A	5 <u>6</u>	IT TECHNICAL SUPPORT SUPERVISOR
2552A	47 <u>19</u>	PRINCIPAL OPERATING SYSTEMS ANALYST
0978A	2 <u>4</u>	PROGRAM MANAGER II
1093A	27 <u>28</u>	SECTION MANAGER,ADMINISTRATION,ISD
6810A	5 <u>3</u>	SECTION MGR,CUSTODIAL SERVICES,ISD
2560A	39 <u>40</u>	SR NETWORK SYSTEMS ADMINISTRATOR
2551A	30 <u>31</u>	SENIOR OPERATING SYSTEMS ANALYST
0913A	49 <u>18</u>	STAFF ASSISTANT II

SECTION 66. Section 6.86.010 (Department of Mental Health) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
8697A	274 <u>273</u>	CLINICAL PSYCHOLOGIST II
8697N	7 <u>8</u>	CLINICAL PSYCHOLOGIST II
8103A	203 <u>211</u>	COMMUNITY WORKER
8103N	2 <u>3</u>	COMMUNITY WORKER
5472J	4 <u>3</u>	CONSULTING SPECIALIST,MD(PER SESS)
1138A	47 <u>16</u>	INTERMEDIATE CLERK
2214N	4 <u>5</u>	INTERMEDIATE TYPIST-CLERK
1848A	48 <u>19</u>	MANAGEMENT ANALYST
9002A	232 <u>237</u>	MEDICAL CASE WORKER II
9002N	4 <u>5</u>	MEDICAL CASE WORKER II
9038A	463 <u>167</u>	MENTAL HEALTH CLINICAL SUPERVISOR
5278A	181 <u>180</u>	MENTAL HEALTH COUNSELOR,RN
4735A	225 <u>226</u>	MENTAL HEALTH PSYCHIATRIST
4735N	4 <u>2</u>	MENTAL HEALTH PSYCHIATRIST
8148A	80 <u>78</u>	MENTAL HEALTH SERVICES COORD I
5856A	3 <u>1</u>	OCCUPATIONAL THERAPIST I
5857A	44 <u>10</u>	OCCUPATIONAL THERAPIST II
5859A	2 <u>1</u>	OCCUPATIONAL THERAPY SUPERVISOR I

9193A	70	<u>69</u>	PATIENT FINANCIAL SERVS WORKER
9192A	64	<u>65</u>	PATIENT RESOURCES WORKER
1331A	6	<u>7</u>	PAYROLL CLERK I
9035A	878	<u>895</u>	PSYCHIATRIC SOCIAL WORKER II
9035F	-48	<u>55</u>	PSYCHIATRIC SOCIAL WORKER II
9035N	35	<u>36</u>	PSYCHIATRIC SOCIAL WORKER II
8162A	-41	<u>47</u>	PSYCHIATRIC TECHNICIAN II
8163A	30	<u>29</u>	PSYCHIATRIC TECHNICIAN III
8593A	14	<u>12</u>	REHABILITATION COUNSELOR II
1140A	45	<u>14</u>	SENIOR CLERK
8105A	25	<u>29</u>	SENIOR COMMUNITY WORKER
0907A	-49	<u>47</u>	STAFF ASSISTANT I
0913A	-42	<u>43</u>	STAFF ASSISTANT II
8242F	24	<u>23</u>	STUDENT WORKER
5884A	-44	<u>47</u>	SUBSTANCE ABUSE COUNSELOR
8712A	-40	<u>39</u>	SUPERVISING PSYCHOLOGIST
1865A	38	<u>39</u>	TRAINING COORDINATOR,MENTAL HEALTH
2201A	9	<u>8</u>	TRANSCRIBER TYPIST

SECTION 67. Section 6.88.010 (Department of Military and Veterans Affairs) is hereby amended to change the number of ordinance positions for the following class:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
8136A	3 <u>5</u>	VETERANS CLAIMS ASSISTANT I

SECTION 68. Section 6.92.010 (Department of Museum of Natural History) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
7959A	4	GRAPHIC ARTIST
2108A	4	MANAGEMENT SECRETARY II
2115A	4	SENIOR MANAGEMENT SECRETARY II

SECTION 69. Section 6.94.010 (Department of Parks and Recreation) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0352F	77 <u>80</u>	GROUPS MAINTENANCE WORKER I
0354A	97 <u>95</u>	GROUPS MAINTENANCE WORKER II
8796H	633 <u>635</u>	RECREATION SERVICES LEADER
8798A	73 <u>72</u>	RECREATION SERVICES SUPERVISOR

SECTION 70. Section 6.100.010 (Probation Department – Support services) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
8612A	4	ASSISTANT PROBATION DIRECTOR
2170A	4	STENOGRAPHER
7139A	4	VIDEO PRODUCTION TECHNICIAN

SECTION 71. Section 6.100.010 (Probation Department – Support services) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>2602A</u>	<u>1</u>	<u>IT SECURITY ANALYST</u>

SECTION 72. Section 6.100.010 (Probation Department – Support services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0578A	25 <u>23</u>	ACCOUNT CLERK II
0647A	5 <u>6</u>	ACCOUNTANT II
0665A	3 <u>2</u>	ACCOUNTING SYSTEMS TECHNICIAN
1881A	5 <u>6</u>	DEPARTMENTAL CIVIL SERVICE REP
1842A	42 <u>16</u>	DEPARTMENTAL PERSONNEL ASSISTANT

8607A	37	<u>41</u>	DEPUTY PROBATION OFFICER II, FIELD
1849A	42	<u>15</u>	SENIOR DEPARTMENTAL PERSONNEL TECH
2547A	44	<u>12</u>	SENIOR IT TECHNICAL SUPPORT ANALYST
2201A	3	<u>2</u>	TRANSCRIBER TYPIST

SECTION 73. Section 6.100.017 (Probation Department – Juvenile institution services) is hereby amended to delete the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
2172A	4	INTERMEDIATE STENOGRAPHER

SECTION 74. Section 6.100.017 (Probation Department – Juvenile institution services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
8612A	44	<u>17</u> ASSISTANT PROBATION DIRECTOR
2201A	34	<u>32</u> TRANSCRIBER TYPIST

SECTION 75. Section 6.100.018 (Probation Department – Field services) is hereby amended to delete the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
2172A	4	INTERMEDIATE STENOGRAPHER

SECTION 76. Section 6.100.018 (Probation Department –Field services) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>8626A</u>	<u>8</u>	<u>TRANSPORTATION DEPUTY, PROBATION</u>

SECTION 77. Section 6.100.018 (Probation Department – Field services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
8607A	4046 <u>1020</u>	DEPUTY PROBATION OFFICER II, FIELD
2214A	308 <u>309</u>	INTERMEDIATE TYPIST-CLERK
2201A	27 <u>24</u>	TRANSCRIBER TYPIST

SECTION 78. Section 6.106.010 (Public Library) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>0739A</u>	<u>1</u>	<u>SENIOR INVENTORY CONTROL ASSISTANT</u>

SECTION 79. Section 6.106.010 (Public Library) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0736A	2 <u>1</u>	INVENTORY CONTROL ASSISTANT II
8334A	177 <u>179</u>	LIBRARIAN I
8337A	43 <u>44</u>	LIBRARIAN IV
8325F	812 <u>818</u>	LIBRARY AID
8326A	185 <u>186</u>	LIBRARY ASSISTANT I
8327A	27 <u>28</u>	LIBRARY ASSISTANT II
9325F	516 <u>521</u>	LIBRARY PAGE,NC

SECTION 80. Section 6.108.010 (Department of Public Social Services) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
8003A	3	COMMUNITY LIAISON WORKER,PSS
9177N	10	ELIGIBILITY WORKER III

SECTION 81. Section 6.108.010 (Department of Public Social Services) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>1002N</u>	<u>1</u>	<u>ADMINISTRATIVE SERVICES MANAGER I</u>
<u>2590N</u>	<u>1</u>	<u>INFORMATION SYSTEMS ANALYST I</u>
<u>2591N</u>	<u>2</u>	<u>INFORMATION SYSTEMS ANALYST II</u>
<u>2603A</u>	<u>2</u>	<u>IT SECURITY SPECIALIST</u>
<u>2594N</u>	<u>1</u>	<u>PRINCIPAL INFO SYSTEMS ANALYST</u>
<u>2525N</u>	<u>2</u>	<u>SENIOR APPLICATION DEVELOPER</u>

SECTION 82. Section 6.108.010 (Department of Public Social Services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0887A	4 <u>18</u>	ADMINISTRATIVE ASSISTANT I

0889A	27	<u>28</u>	ADMINISTRATIVE ASSISTANT III
1002A	403	<u>108</u>	ADMINISTRATIVE SERVICES MANAGER I
2521A	42	<u>13</u>	APPLICATION DEVELOPER II
1182A	43	<u>45</u>	CHIEF CLERK
4229A	53	<u>45</u>	CONTRACT PROGRAM MONITOR
9181A	934	<u>935</u>	ELIGIBILITY SUPERVISOR
9181N	6	<u>3</u>	ELIGIBILITY SUPERVISOR
9179N	22	<u>1</u>	ELIGIBILITY WORKER II
9177A	434	<u>422</u>	ELIGIBILITY WORKER III
9166A	463	<u>168</u>	GAIN SERVICES SUPERVISOR
9165A	964	<u>1000</u>	GAIN SERVICES WORKER
8021A	294	<u>301</u>	HUMAN SERVICES ADMINISTRATOR I
8021N	5	<u>6</u>	HUMAN SERVICES ADMINISTRATOR I
8023A	73	<u>74</u>	HUMAN SERVICES ADMINISTRATOR III
2591A	98	<u>99</u>	INFORMATION SYSTEMS ANALYST II
2546A	6	<u>7</u>	IT TECHNICAL SUPPORT ANALYST II
2214A	2017	<u>1926</u>	INTERMEDIATE TYPIST-CLERK
1848A	27	<u>71</u>	MANAGEMENT ANALYST
2526A	8	<u>9</u>	PRINCIPAL APPLICATION DEVELOPER
7980A	457	<u>172</u>	PROGRAM ASSISTANT,PSS
2095A	143	<u>146</u>	SECRETARY II
2097A	74	<u>69</u>	SECRETARY IV

2525A	17	<u>19</u>	SENIOR APPLICATION DEVELOPER
1140A	239	<u>218</u>	SENIOR CLERK
1849A	3	<u>6</u>	SENIOR DEPARTMENTAL PERSONNEL TECH
2593A	36	<u>35</u>	SENIOR INFORMATION SYSTEMS ANALYST
2547A	40	<u>11</u>	SENIOR IT TECHNICAL SUPPORT ANALYST
2560A	13	<u>15</u>	SR NETWORK SYSTEMS ADMINISTRATOR
2101A	23	<u>28</u>	SENIOR SECRETARY II
0913A	44	<u>15</u>	STAFF ASSISTANT II
9128N	4	<u>2</u>	STAFF DEVELOPMENT SPEC,WELFARE

SECTION 83. Section 6.109.010 (Department of Public Works) is hereby amended to delete the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
6336A	2	GUNITE GUN OPERATOR
6338A	4	GUNITE NOZZLE OPERATOR
2214F	4	INTERMEDIATE TYPIST-CLERK

SECTION 84. Section 6.109.010 (Department of Public Works) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1007A	4	<u>2</u> ADMINISTRATIVE SERVICES DIV MGR

3433A	266	<u>272</u>	ASSOCIATE CIVIL ENGINEER
6774A	25	<u>20</u>	CUSTODIAN
6492A	20	<u>21</u>	ELECTRO-MECHANIC
3606A	9	<u>5</u>	ENGINEERING AID II
3608A	34	<u>37</u>	ENGINEERING AID III
4371A	11	<u>10</u>	ENGINEERING GEOLOGIST
3856A	-4	<u>3</u>	ENGINEERING TESTING AID III
6012A	2	<u>3</u>	GARAGE ATTENDANT I
7379A	5	<u>4</u>	HEAVY POWER EQUIPMENT OILER
6349A	47	<u>16</u>	HELPER,ELECTRICAL
3683A	6	<u>5</u>	HIGHWAY TECHNICIAN
2574A	3	<u>2</u>	INFORMATION TECHNOLOGY MANAGER III
1138A	20	<u>19</u>	INTERMEDIATE CLERK
2214A	402	<u>101</u>	INTERMEDIATE TYPIST-CLERK
7077A	4	<u>2</u>	PHOTOGRAPHER II
7374A	50	<u>53</u>	POWER EQUIPMENT OPERATOR
7427A	24	<u>20</u>	POWER EQUIPMENT TECH HELPER II
3430A	468	<u>170</u>	PRINCIPAL CIVIL ENGINEERING ASST
3671A	47	<u>19</u>	PRINCIPAL CIVIL ENGINEERING TECH
0977A	7	<u>8</u>	PROGRAM MANAGER I
0978A	40	<u>12</u>	PROGRAM MANAGER II
5924A	414	<u>116</u>	PUBLIC WORKS CREW LEADER

5922A	413	<u>111</u>	PUBLIC WORKS LABORER
5923A	319	<u>320</u>	PUBLIC WORKS MAINTENANCE WORKER
2097A	44	<u>43</u>	SECRETARY IV
1140A	22	<u>21</u>	SENIOR CLERK
1849A	9	<u>10</u>	SENIOR DEPARTMENTAL PERSONNEL TECH
3621A	24	<u>23</u>	SENIOR SURVEY-MAPPING TECHNICIAN
2216A	28	<u>30</u>	SENIOR TYPIST-CLERK
8243F	75	<u>76</u>	STUDENT PROFESSIONAL WORKER I
0394A	7	<u>8</u>	TREE TRIMMER WORKING SUPERVISOR
9347F	3	<u>2</u>	TRUCK CRANE OILER(OAA),NC

SECTION 85. Section 6.112.010 (Department of Regional Planning) is hereby amended to change the number of ordinance positions for the following class:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
4431A	25 <u>26</u>	SENIOR REGIONAL PLANNING ASSISTANT

SECTION 86. Section 6.120.010 (Sheriff – Administration) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>1031A</u>	<u>1</u>	<u>HEAD COMPLIANCE OFFICER</u>

SECTION 87. Section 6.120.010 (Sheriff – Administration) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1002A	30 <u>31</u>	ADMINISTRATIVE SERVICES MANAGER I
2721A	5 <u>6</u>	CAPTAIN
2723A	4 <u>5</u>	COMMANDER
0684A	4	<u>7</u> COMPLIANCE AUDITOR
2708A	62 <u>63</u>	DEPUTY SHERIFF
1924A	57 <u>59</u>	EMPLOYMENT SERVS ASST II,SHERIFF
2745A	8	<u>10</u> LAW ENFORCEMENT TECHNICIAN
2719A	47 <u>23</u>	LIEUTENANT
1228A	44	<u>13</u> OPERATIONS ASSISTANT I,SHERIFF
1229A	40	<u>12</u> OPERATIONS ASSISTANT II,SHERIFF
1230A	20	<u>26</u> OPERATIONS ASSISTANT III,SHERIFF
2098A	7 <u>8</u>	SECRETARY V
2104A	4	<u>2</u> SENIOR SECRETARY V
2717A	43 <u>69</u>	SERGEANT
8243F	20 <u>21</u>	STUDENT PROFESSIONAL WORKER I
8242F	402 <u>100</u>	STUDENT WORKER

SECTION 88. Section 6.120.011 (Sheriff – Court services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
2708A	4324 <u>1320</u>	DEPUTY SHERIFF
2708N	44 <u>43</u>	DEPUTY SHERIFF
8242F	3 <u>5</u>	STUDENT WORKER

SECTION 89. Section 6.120.012 (Sheriff – Custody) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>1750A</u>	<u>1</u>	<u>STATISTICAL ANALYST,SHERIFF</u>

SECTION 90. Section 6.120.012 (Sheriff – Custody) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
2721A	40 <u>11</u>	CAPTAIN
2708A	2629 <u>2637</u>	DEPUTY SHERIFF
6875A	43 <u>12</u>	LAUNDRY SUPERVISOR I
2719A	78 <u>88</u>	LIEUTENANT
1228A	32 <u>33</u>	OPERATIONS ASSISTANT I,SHERIFF

2098A	44	<u>12</u>	SECRETARY V
2717A	247	<u>317</u>	SERGEANT
2331A	45	<u>16</u>	WAREHOUSE WORKER I

SECTION 91. Section 6.120.013 (Sheriff – Detective services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.		NO. OF ORDINANCE POSITIONS	TITLE
2708A	520	<u>523</u>	DEPUTY SHERIFF
2717A	434	<u>132</u>	SERGEANT

SECTION 92. Section 6.120.014 (Sheriff – General support services) is hereby amended to delete the following class and number of ordinance positions:

ITEM NO.		NO. OF ORDINANCE POSITIONS	TITLE
1924A	2		EMPLOYMENT SERVS ASST II, SHERIFF

SECTION 93. Section 6.120.014 (Sheriff – General support services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.		NO. OF ORDINANCE POSITIONS	TITLE
1002A	3	<u>5</u>	ADMINISTRATIVE SERVICES MANAGER I
1003A	2	<u>3</u>	ADMINISTRATIVE SERVICES MANAGER II

6547A	19	<u>21</u>	AUDIO,VIDEO,& SEC SYST TECHNICIAN
2708A	233	<u>243</u>	DEPUTY SHERIFF
1138A	40	<u>11</u>	INTERMEDIATE CLERK
8700A	7	<u>9</u>	LAW ENFORCEMENT PSYCHOLOGIST,SHER
2745A	-44	<u>47</u>	LAW ENFORCEMENT TECHNICIAN
2719A	36	<u>41</u>	LIEUTENANT
1228A	38	<u>40</u>	OPERATIONS ASSISTANT I,SHERIFF
1229A	-44	<u>43</u>	OPERATIONS ASSISTANT II,SHERIFF
1230A	-44	<u>42</u>	OPERATIONS ASSISTANT III,SHERIFF
2717A	407	<u>135</u>	SERGEANT
1750A	-4	<u>5</u>	STATISTICAL ANALYST,SHERIFF
8243F	9	<u>8</u>	STUDENT PROFESSIONAL WORKER I

SECTION 94. Section 6.120.016 (Sheriff – County services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.		NO. OF ORDINANCE POSITIONS	TITLE
2708A	225	<u>231</u>	DEPUTY SHERIFF
2745A	57	<u>56</u>	LAW ENFORCEMENT TECHNICIAN
2719A	48	<u>17</u>	LIEUTENANT
2717A	78	<u>77</u>	SERGEANT

SECTION 95. Section 6.120.018 (Sheriff – Patrol clearing account) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
2708A	3674 <u>3673</u>	DEPUTY SHERIFF
2708N	88 <u>89</u>	DEPUTY SHERIFF
2745A	316 <u>321</u>	LAW ENFORCEMENT TECHNICIAN
2719A	477 <u>179</u>	LIEUTENANT
1228A	44 <u>15</u>	OPERATIONS ASSISTANT I, SHERIFF
2717A	642 <u>643</u>	SERGEANT

SECTION 96. Section 6.126.010 (Treasurer and Tax Collector) is hereby amended to delete the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1261A	2	OPERATIONS SPEC, BANK & REMIT PROC

SECTION 97. Section 6.126.010 (Treasurer and Tax Collector) is hereby amended to add the following classes and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
<u>8258F</u>	<u>3</u>	<u>STUDENT PROFESSIONAL WORKER II</u>
<u>2481F</u>	<u>1</u>	<u>STUDENT WORKER, INFO TECH</u>

SECTION 98. Section 6.126.010 (Treasurer and Tax Collector) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
0577A	33 <u>32</u>	ACCOUNT CLERK I
0647A	20 <u>19</u>	ACCOUNTANT II
0642A	24 <u>20</u>	ACCOUNTING TECHNICIAN I
0487A	3 <u>2</u>	PRINCIPAL CASH SYSTEMS ANALYST
0913A	2 <u>3</u>	STAFF ASSISTANT II
8243F	48 <u>19</u>	STUDENT PROFESSIONAL WORKER I
1367A	73 <u>71</u>	TAX SERVICES CLERK II
2331A	2 <u>4</u>	WAREHOUSE WORKER I

SECTION 99. Pursuant to Government Code Section 25123(f), this ordinance shall take effect no earlier than July 1, 2014. If this ordinance becomes effective after July 1, 2014, it shall be construed and applied as if it were effective and operative on and after July 1, 2014.

*The Executive Office/Clerk of the Board of Supervisors shall insert the effective date for the salary or salary schedule and level in the space provided for the classification added and compensation changes to Section 6.28.050 of the County Code.

[FY2014-2015RECBUDGABCEO]

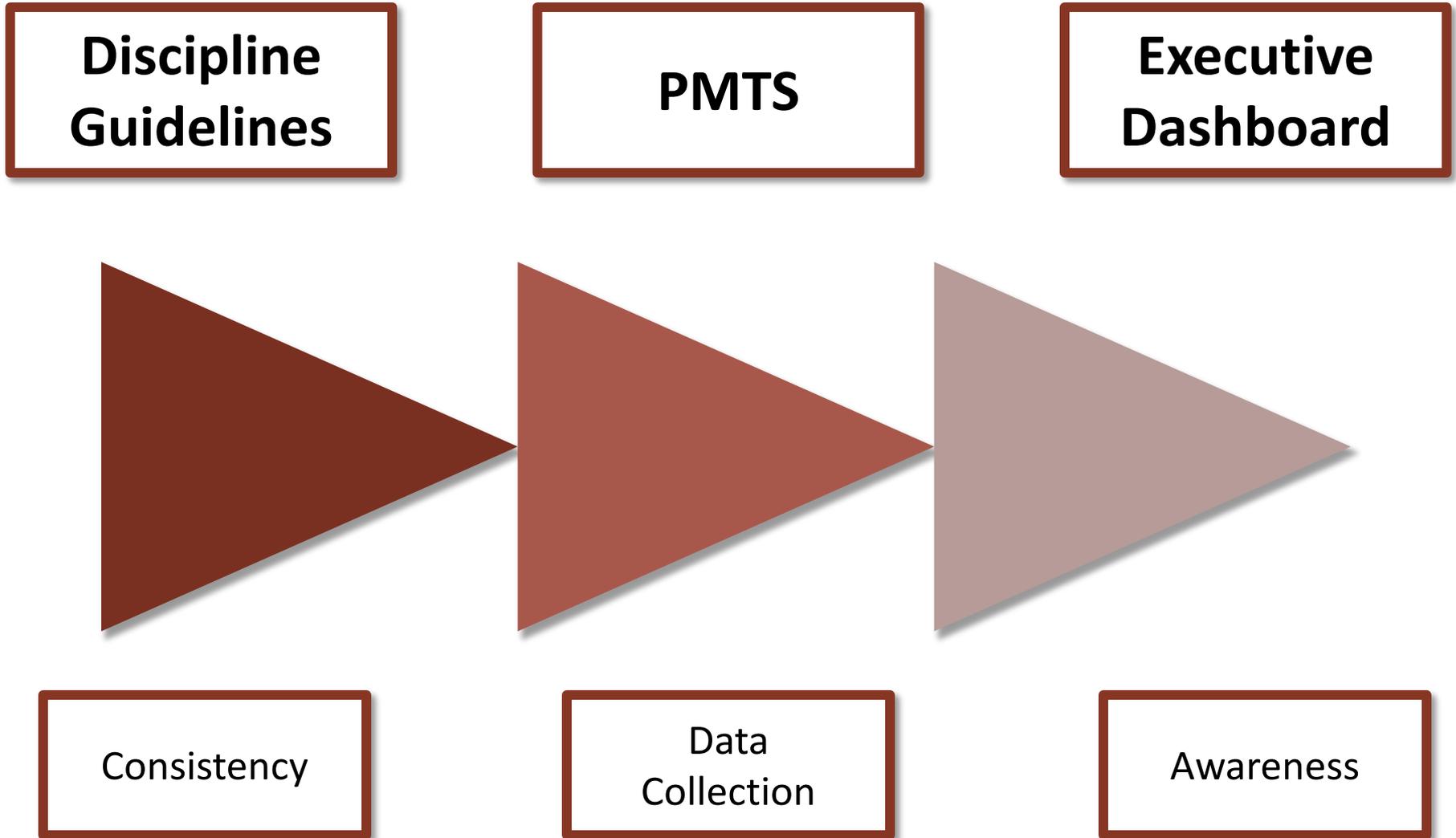
Performance Mgmt. Tracking System (PMTS)

DASHBOARDS

Operations Cluster Meeting
05/08/2014

"Automate all things HR..."

Performance Management - An Integrated Approach



"Automate all things HR..."

PMTS Overview

A

Implemented on June 30, 2012

B

Enables departments to track and manage administrative matters related to employee discipline

C

Serves as a central repository that provides ready access to data or metrics across County departments

D

Seamlessly integrates with County's eHR

"Automate all things HR..."

Post Implementation Status

- Thirty one departments live
- Historical cases migrated to PMTS = 8,410 records
 - Five legacy systems retired
- New cases since July 1, 2012 = 4,724 records

"Automate all things HR..."



Process Change



LISA M. GARRETT
DIRECTOR OF PERSONNEL

COUNTY OF LOS ANGELES DEPARTMENT OF HUMAN RESOURCES

HEADQUARTERS
579 KENNETH HAHN HALL OF ADMINISTRATION • LOS ANGELES, CALIFORNIA 90012
(213) 974-2406 FAX (213) 621-0387

BRANCH OFFICE
3333 WILSHIRE BOULEVARD • LOS ANGELES, CALIFORNIA 90010
(213) 738-2211 FAX (213) 637-0820

June 5, 2013

To: All Departmental Human Resources Managers

From: Epifanio Peinado 
Assistant Director

Subject: **PERFORMANCE MANAGEMENT TRACKING SYSTEM AND DASHBOARD**

The Performance Management Tracking System (PMTS) began countywide implementation on June 30, 2012. PMTS is now the central repository for all performance management matters and related discipline in the County of Los Angeles. We are pleased to report that the majority of County departments are currently utilizing the system. However, we need to make more progress by ensuring that data is timely and continuously inputted into the system. Additionally, we are moving forward in developing countywide and departmental dashboards based on available PMTS data for use by human resources professionals and departmental executives.

“all letters of intent to discharge and probationary actions referred to DHR Advocacy must be entered into PMTS”

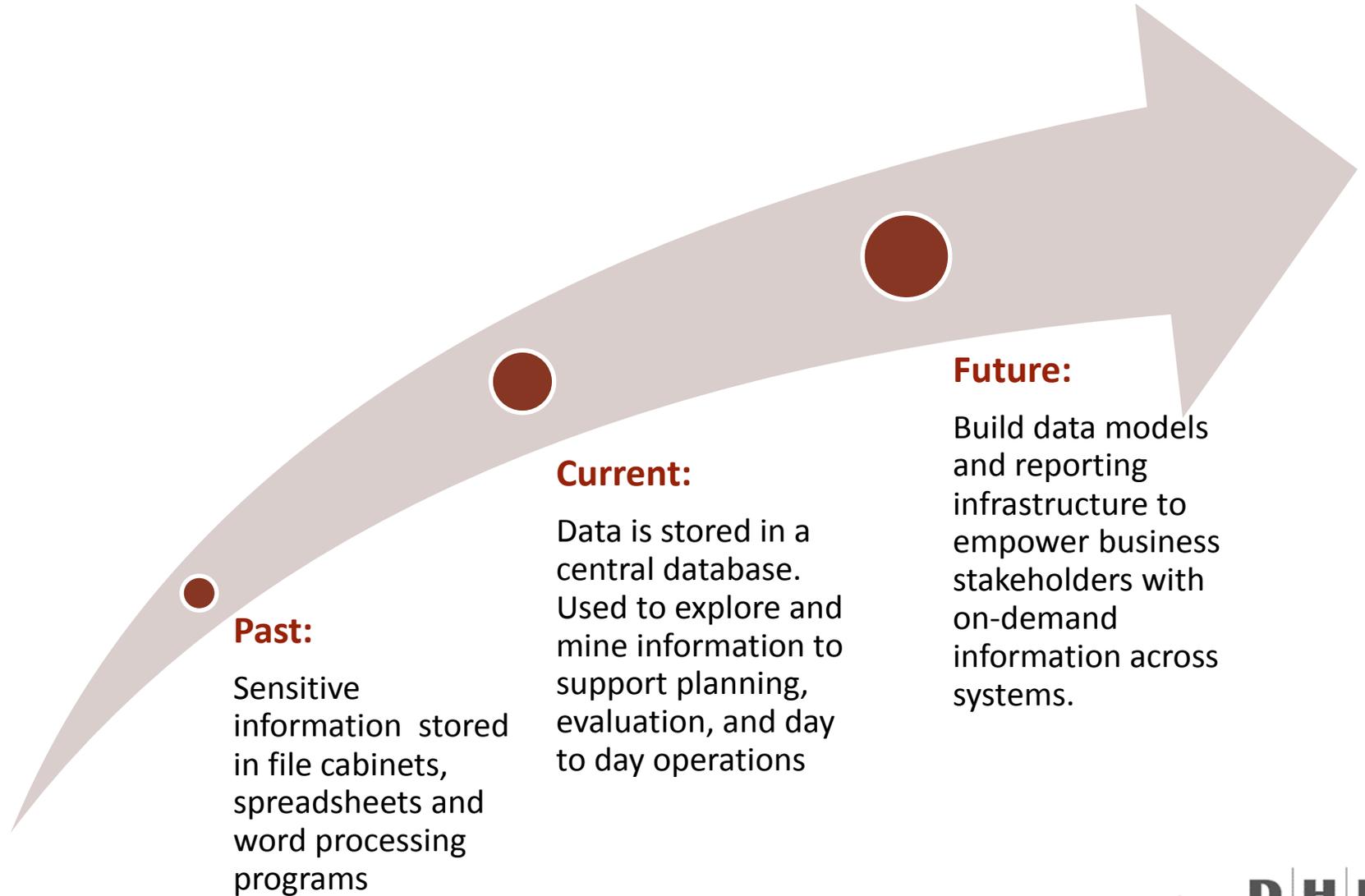
“Automate all things HR...”



D | H | R

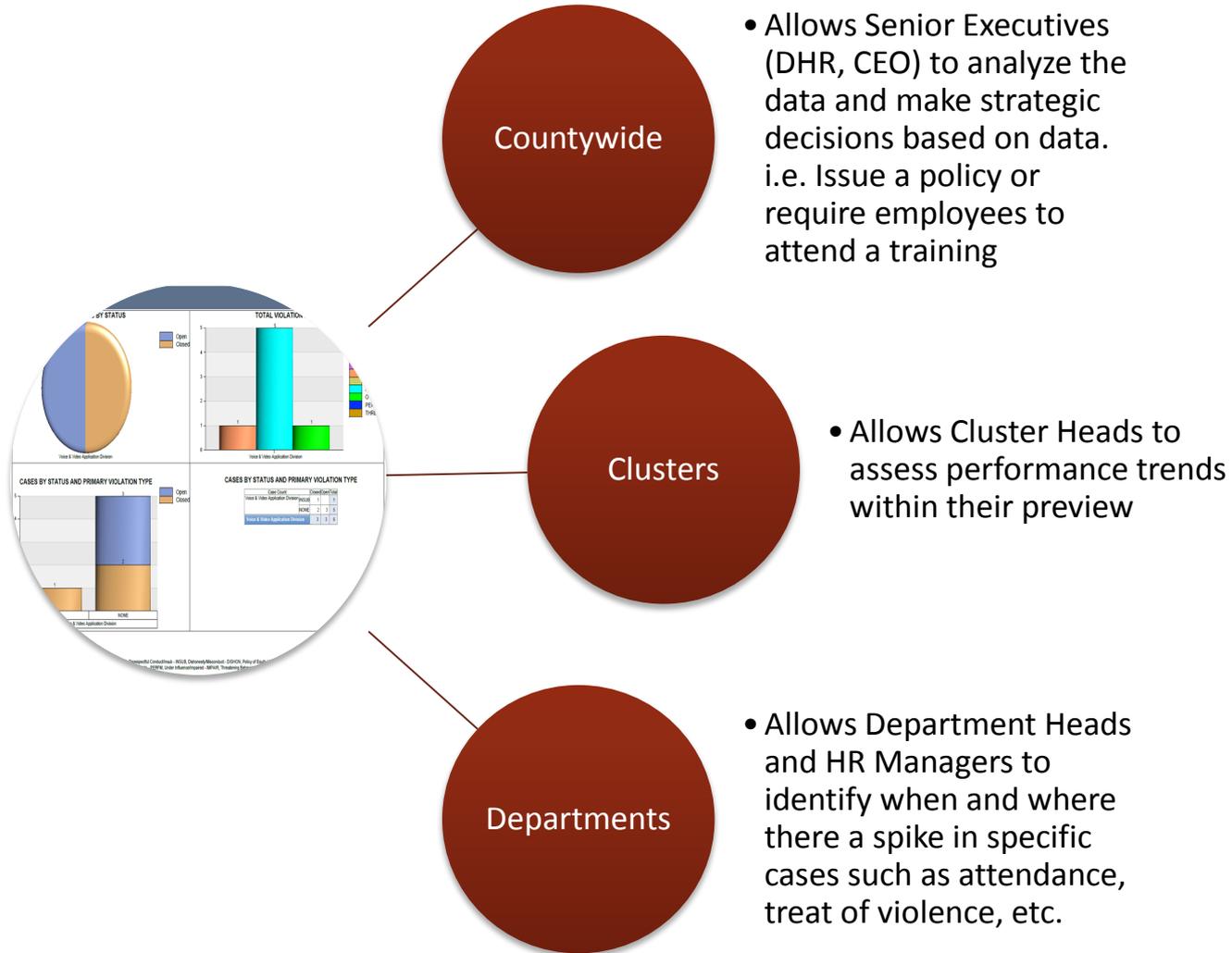
Department of Human Resources
County of Los Angeles

Fact-Based Decision Making

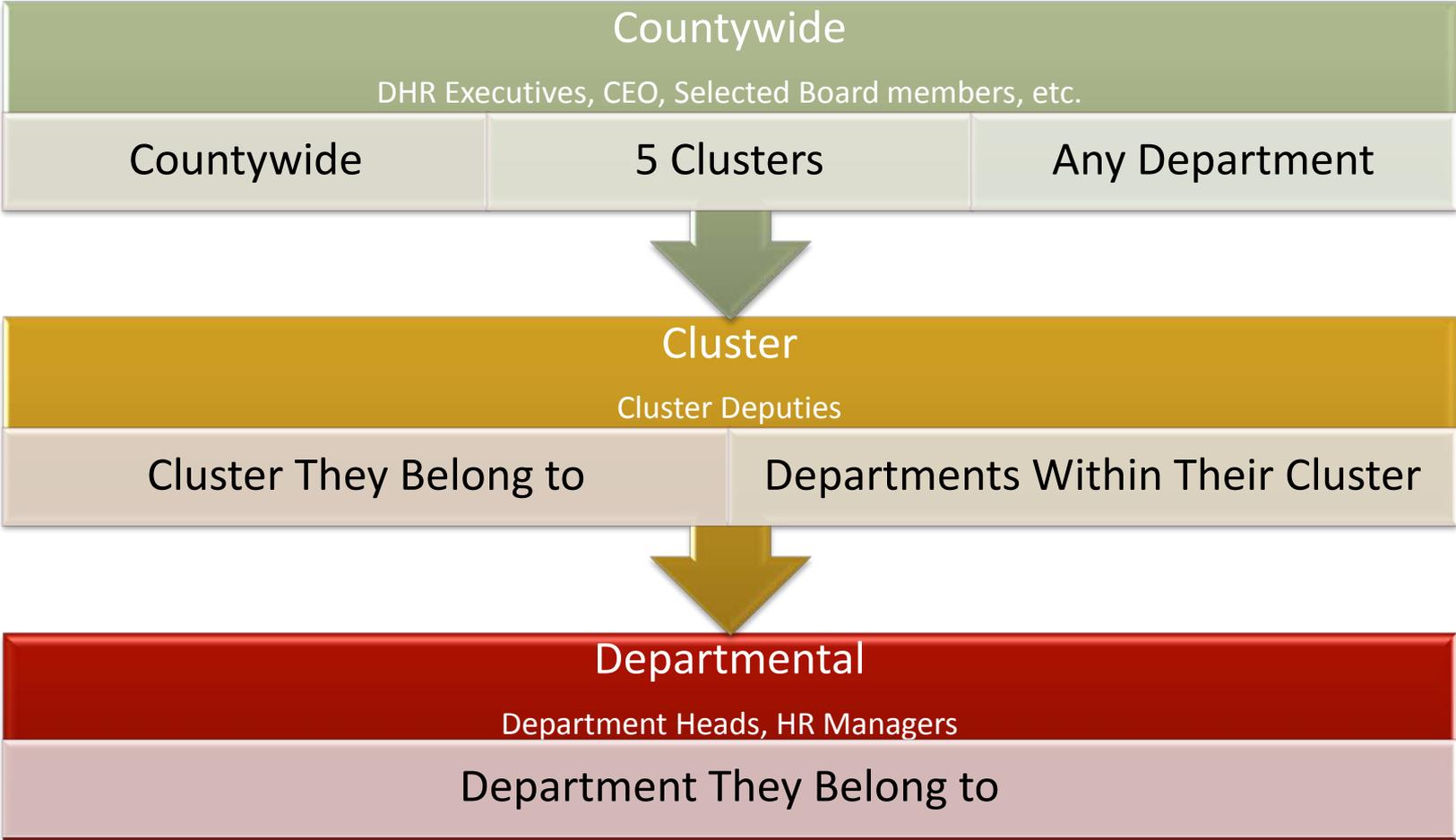


"Automate all things HR..."

Case Status by Violation Type

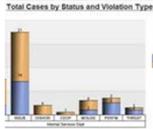


Access Level



"Automate all things HR..."

Future Dashboard Deployment



Case Status by Violation Type



Cases by Violation Type and Corresponding Disciplinary Action **(In Development)**



Cases by Employee Characteristics by Violation Type **(In Development)**



Cases by Appeal Type (CSC, ERCOM, etc.)

- View Final Outcome of Cases



Cycle Times

- Allow Users to Determine if Standards are Being Met

Countywide View (Test Data)

DHR Department of Human Resources
Info

CASES BY STATUS

CountyWide

TOTAL VIOLATION BY TYPE

Fiscal Year

Current Fiscal Year ▼

Q 1
 Q 2
 Q 3
 Q 4

[Select all](#) [Deselect all](#)

Select Status

Closed
 Open

[Select all](#) [Deselect all](#)

Select Violation Code

Attendance - ATTND
 Criminal/Unbecoming Conduct - CRIML
 Dishonesty/Misconduct - DISHON
 Disrespectful Conduct/Insub - INSUB
 Misuse of County Property - MISUSE
 Other - OTHER
 Performance to Standards - PERFM
 Policy of Equity Violation - CEOP
 Threatening Behavior - THREAT
 Under Influence/Impaired - IMPAIR

[Select all](#) [Deselect all](#)

CASES BY STATUS AND PRIMARY VIOLATION TYPE

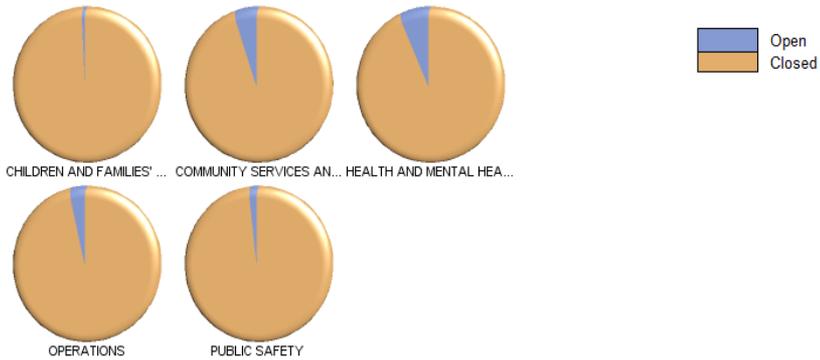
CountyWide

CASES BY STATUS AND PRIMARY VIOLATION TYPE

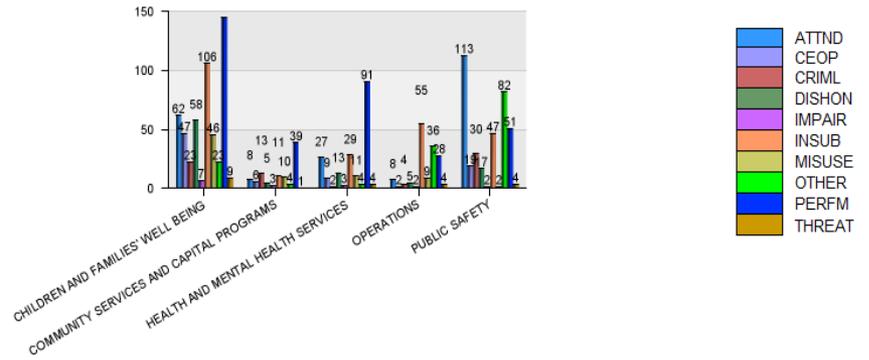
Case Count	Closed	Open	Total	
CountyWide	ATTND	212	1	213
CEOP	57	4	61	
CRIML	60	1	61	
DISHON	67	2	69	
IMPAIR	16	1	17	
INSUB	162	6	168	
MISUSE	67		67	
OTHER	82	3	85	
PERFM	267	8	275	
THREAT	13		13	

Cluster View (Test Data)

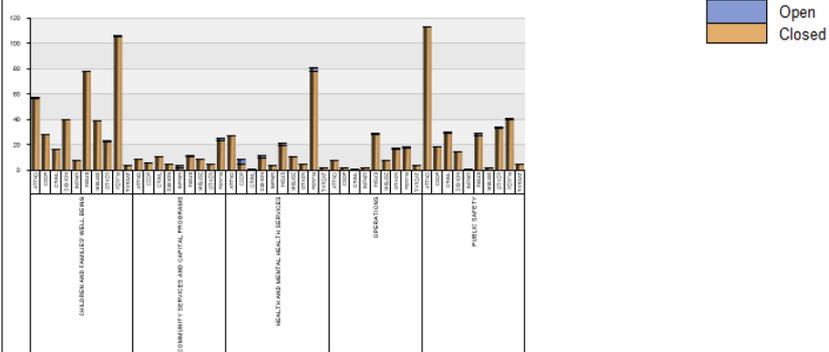
CASES BY STATUS



TOTAL VIOLATION BY TYPE



CASES BY STATUS AND PRIMARY VIOLATION TYPE



CASES BY STATUS AND PRIMARY VIOLATION TYPE

Case Count		Closed	Open	Total
CHILDREN AND FAMILIES' WELL BEING				
ATTND	56	1	57	
CEOP	28		28	
CRIML	16		16	
DISHON	40		40	
IMPAIR	7		7	
INSUB	78		78	
MISUSE	39		39	
OTHER	22	1	23	
PERFM	105	1	106	
THREAT	3		3	

Cluster View - First Quadrant (Test Data)

CASES BY STATUS

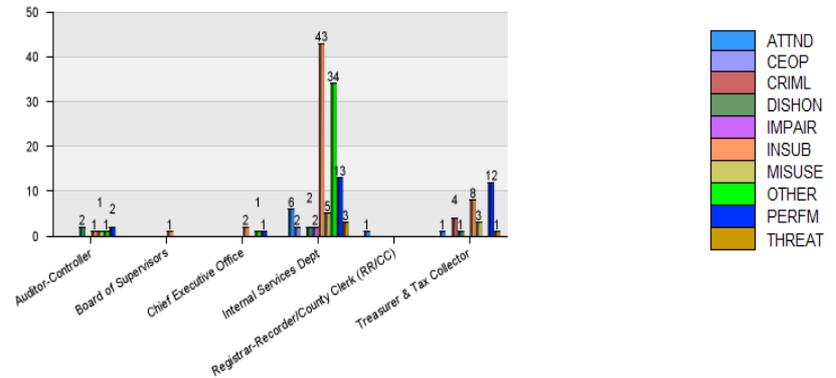


Level 1 Organizations Operations Cluster (Test Data)

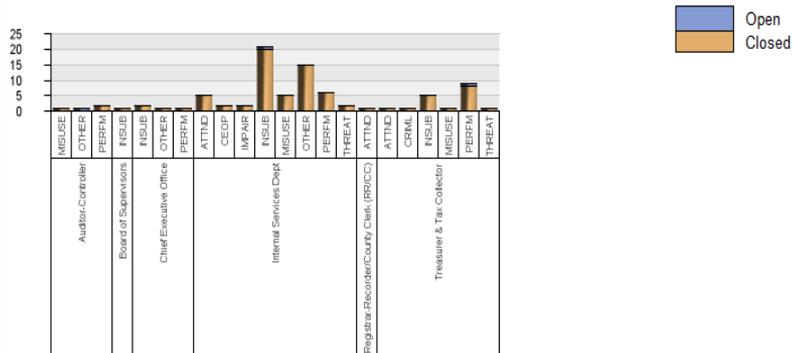
CASES BY STATUS



TOTAL VIOLATION BY TYPE



CASES BY STATUS AND PRIMARY VIOLATION TYPE

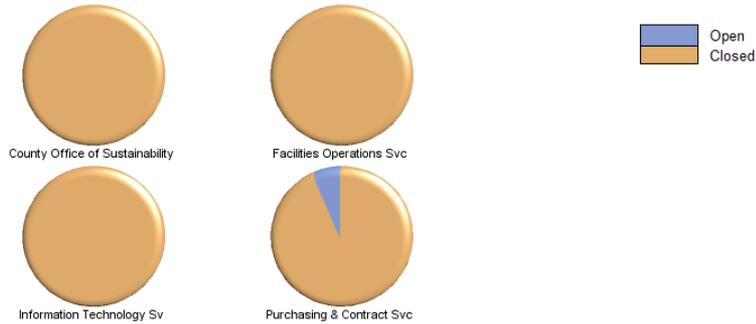


CASES BY STATUS AND PRIMARY VIOLATION TYPE

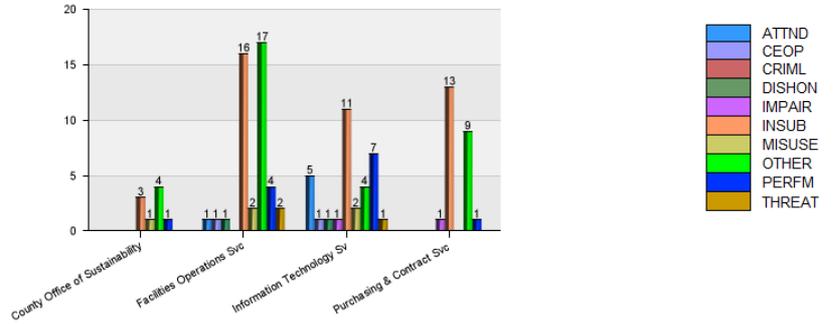
Case Count		Closed	Open	Total
Auditor-Controller	MISUSE	1	0	1
	OTHER	0	1	1
	PERFM	2	0	2
	SubTotal	3	1	4
Board of Supervisors	INSUB	1	0	1
	SubTotal	1	0	1
Chief Executive Office	INSUB	2	0	2
	OTHER	1	0	1
	PERFM	1	0	1
	SubTotal	4	0	4

ISD - Level 2 Organizations (Test Data)

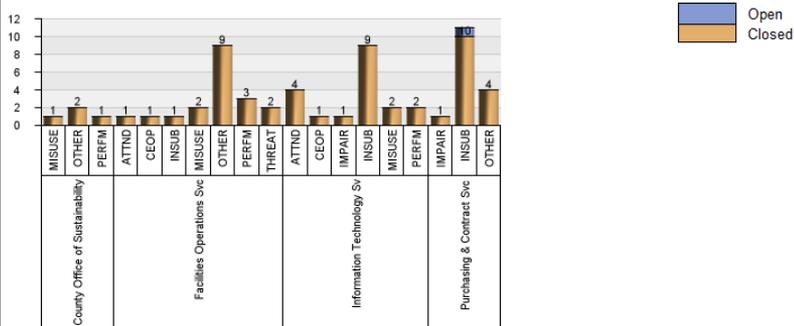
CASES BY STATUS



TOTAL VIOLATIONS BY TYPE



CASES BY STATUS AND PRIMARY VIOLATION TYPE



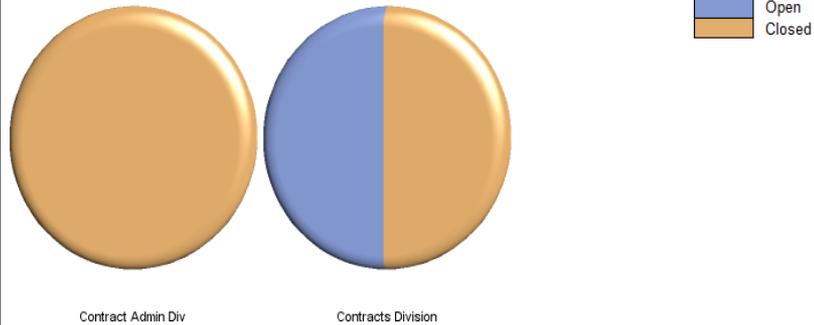
CASES BY STATUS AND PRIMARY VIOLATION TYPE

Case Count		Closed	Open	Total
County Office of Sustainability	MISUSE	1	0	1
	OTHER	2	0	2
	PERFM	1	0	1
	SubTotal	4	0	4
Facilities Operations Svc	ATTND	1	0	1
	CEOP	1	0	1
	INSUB	1	0	1
	MISUSE	2	0	2
	OTHER	9	0	9
	PERFM	3	0	3

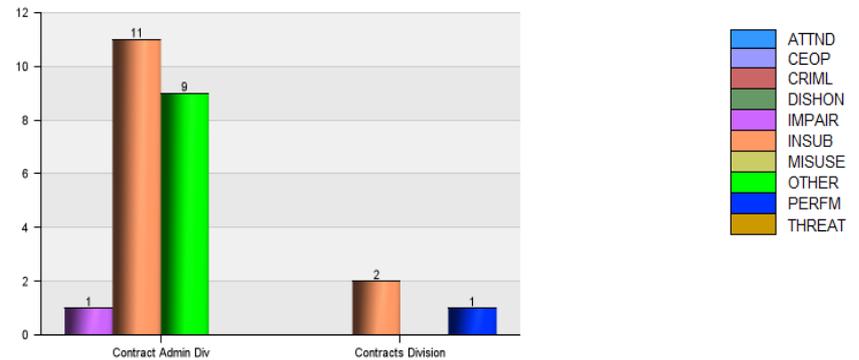
ISD

Level 3 Organizations Within Purchasing and Contract Services (Test Data)

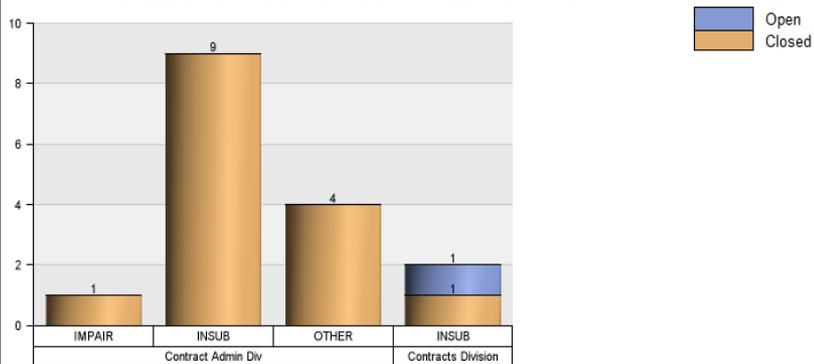
CASES BY STATUS



TOTAL VIOLATIONS BY TYPE



CASES BY STATUS AND PRIMARY VIOLATION TYPE



CASES BY STATUS AND PRIMARY VIOLATION TYPE

Case Count		Closed	Open	Total
Contract Admin Div	IMPAIR	1	0	1
	INSUB	9	0	9
	OTHER	4	0	4
	SubTotal	14	0	14
Contracts Division	INSUB	1	1	2
	SubTotal	1	1	2
Purchasing & Contract Svc		15	1	16

Summary of Proposed Revisions to IT Security Policies 6.100 – 6.112

Policy 6.100 – Information Technology and Security Policy

- ✓ Clarifications and updates to reflect use of mobile computers and adherence to IT security technical and operational standards and procedures approved by the Information Security Steering Committee.
- ✓ Added reference to California Civil Code Section 1798.29 regarding breach notifications.
- ✓ Added digital content to include video recordings, photographs, and electronically stored information.
- ✓ Requires designation of a back-up to the Department Information Security Officer.

Policy 6.101 – Use of County Information Technology Resources

- ✓ Added reference to County Policy 9.015 – County Policy of Equity.
- ✓ Clarifications and updates regarding no privacy expectations for use of County IT Resources and inappropriate use of County IT resources.
- ✓ Added monitoring of electronic communications using County IT Resources.
- ✓ Requires use of two-factor authentication for all remote access to County personal and confidential information.

Policy 6.102 – Countywide Antivirus Security Policy

- ✓ Added references to relevant Board IT Security Policies and requirement for remote users to have antivirus protection on personal equipment used to access County IT Resources.

Policy 6.103 – Countywide Computer Security Threat Responses

- ✓ Clarifications and updates regarding preservation of evidence to facilitate administration of justice to protect County IT Resources.

Policy 6.104 – Electronic Communications

- ✓ Clarifications and updates to expand policy to include additional forms of electronic communications, e.g. instant messaging, no expectation of privacy in the use of County IT Resources, and monitoring use of County IT Resources are in accordance with applicable policies and laws.
- ✓ Added reference to County Policy 9.015 – County Policy of Equity.

Policy 6.105 – Internet Usage Policy

- ✓ Added reference to County Policy 9.015 – County Policy of Equity
- ✓ Clarifications and updates to inappropriate use of County IT Resources, requirements for use of social media, and no expectation of privacy for use of County IT Resources.

Policy 6.106 – Physical Security

- ✓ No changes other than extending sunset review date.

Policy 6.107 – Information Technology Risk Assessment

- ✓ Minor revision to provide examples of items to be included in an IT risk assessment program, e.g. vulnerability scans of networks, systems and applications.

Policy 6.108 – Auditing and Compliance

- ✓ No changes other than extending sunset review date.

Policy 6.109 – Security Incident Reporting

- ✓ Added references to California Civil Code Section 1798.29 regarding breach notifications and Code of Federal Regulations 160.103 regarding Protected Health Information.
- ✓ Clarifications and updates to include additional examples of security incidents and reference.

Policy 6.110 – Protection of Information on Portable Computing Devices

- ✓ Added references to HIPAA 1996, HITECH 2009 and California Civil Code Section 1798.29, as well as relevant IT Security Policies.
- ✓ Requires approval of County department management to place personal and/or confidential information on portable computing devices and encryption of such information stored on portable computing devices.

Policy 6.111 – Information Security Awareness Training

- ✓ Added reference to County Policy 9.015 – County Policy of Equity.
- ✓ Minor clarifications regarding awareness training in support of information security policies.

Policy 6.112 – Secure Disposition of Computing Devices

- ✓ Update to require vendor certification for disposition of computing devices in accordance to County security policy requirements.



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) security program supported by countywide policies within the Board of Supervisors Policy Manual (Manual) chapter 6 including related policies (e.g., chapters 3, 7, and 9) in other chapters of the Manual (e.g., chapters 3, 7, and 9) -in-order to assure appropriate and authorized access, usage, and ~~the~~ integrity of County 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

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

[California Civil Code Section 1798.29](#)

POLICY

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 are portable computing devices that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to the County's IT resources; and
 - Mobile computers that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to County IT resources; and infrastructure and/or application system(s)
 - Portable devices, including, without limitation, personal digital assistants (PDAs), digital cameras, smartphones, cell phones, and pagers, wearable computers (also known as body-borne computers or wearables), 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; and
 - Multiple user and application computers, including, without limitation, servers
 - Printing and scanning devices, including, without limitation, printers, copiers, scanners, and fax machines
 - 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, and stored instructions
- Information, including, without limitation, the following:
 - Data
 - Documentation
 - Electronic communications mail (e.g., email, text message)
 - Personal information
 - Confidential information
 - Voice recordings

- Photographs
- Electronically stored information (data that is created, altered, communicated and stored in digital form)

- 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, exposure, loss, or ~~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 ~~and~~ the CIO, in consultation with ~~and~~ County Counsel, 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 access, use, exposure, disclosure, and modification

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

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 Officer (CIO)

The Chief Information Office shall ensure the development of countywide County IT resources policies, standards, and procedures and countywide County IT security policies, standards, and procedures. These County IT security policies shall include, without limitation, the appropriate [access, use, exposure, disclosure, and modification](#) of County IT resources for internal and external activities (e.g., email and other [electronic](#) communications, and Internet access and use). When approved, these policies shall be published and made available to all County IT users to ensure their awareness and compliance.

Chief Information Security Officer (CISO)

The CISO shall report to the CIO and is responsible for the Countywide Information Security Program. The responsibilities of the CISO include, without limitation, the following:

- Developing and maintaining the Countywide Information Security Strategic Plan
- Chairing the Information Security Steering Committee (ISSC)
- Providing County IT security-related technical, regulatory, and policy leadership

- Facilitating the implementation of County IT security policies
- Coordinating County IT security efforts across organizational boundaries
- Leading County IT security training and education efforts
- Directing the Countywide Computer Emergency Response Team (CCERT)

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 County IT resources within the County Department
- 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 technical and operational security standards and procedures approved by the ISSC
- Ensure that County IT resources are implemented and configured to meet County IT security technical and operational standards and procedures approved by the ISSC
- Ensure that County IT resources are maintained at current critical security patch levels
- Implement IT-based services that adhere to all applicable County IT resources policies, standards, and procedures and County IT security policies, standards, and procedures

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 County IT resources within the County Department
- Assist in the development of County Department IT security policies
- Regularly represent the County Department at the ISSC meetings and related activities
- Lead the Departmental Computer Emergency Response Team (DCERT)
- Ensure the County Department is regularly represented at the CCERT meetings and related activities
- Ensure the County Department is regularly represented at the Security Engineering Teams (SET) meetings and related activities
- Report County IT security incidents to the CISO, as required by County IT security policies, standards, and procedures

County IT Users

County IT users are responsible for acknowledging and adhering to County IT resources policies, standards, and procedures and County IT security policies. They are responsible for the following:

- Protection of County IT resources for which they are entrusted; accessing, using, exposing, disclosing, and modifying County IT resources only as authorized; and a-accessing and using them for their intended purposes;
- County IT users are required to sign the “Acceptable Use Agreement” as a condition of being granted access to County IT resources. The Acceptable Use Agreement is set forth in Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources.

Countywide Computer Emergency Response Team (CCERT)

[Include Definition?]

Departmental Computer Emergency Response Team (DCERT)

[Include definition?]

Information Security Steering Committee (ISSC)

The ISSC is established to be the coordinating body for all County IT security-related activities and is composed of the DISO (or Assistant DISO), from all County Departments.

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

- Assisting the CISO in developing, reviewing, and recommending countywide County IT security policies
- Identifying and recommending industry best practices for countywide County IT security
- Developing, reviewing, recommending, and approving countywide County IT security technical and operational standards, procedures, and guidelines
- Coordinating communication and collaboration among County Departments on countywide and County Department IT security issues
- Coordinating countywide County 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 shall be reviewed by the CISO and the CIO, and shall require approval by the Board. 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 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

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 for use of County information technology (IT) resources.

REFERENCE

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. 6.109 – Security Incident Reporting

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

[Board of Supervisors Policy No. 9.015 – County Policy of Equity](#)

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

[California Civil Code Section 1798.29](#)

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 acknowledge and adhere to County IT resources policies, standards, and procedures and County IT security policies and shall sign ~~an~~the Acceptable Use Agreement attached to this Board of Supervisors Policy No. 6.101, prior to being granted access to County IT resources, and annually thereafter.

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. Having no expectation to any right to privacy includes, for example, that County IT users' access and use of County IT resources may be monitored or investigated by authorized persons at any time, without notice or consent.

Activities of County IT users may be logged/stored, ~~are~~ may be 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 accessed and used only for County County management approved business purposes that have been approved by designated County Department management only; unlessexcept expressly authorized by Board of Supervisors' Policy No. 6.105 – Internet Usage.

County IT resources, may not be used:

- For any unlawful purpose;
- For any purpose detrimental to the County or its interests;
- For personal financial gain;
- In any way that undermines or interferes with access to or use of County IT resources for official County purposes;
- In any way that hinders productivity, efficiency, customer service, or interferes with a County IT user's performance of his/her official job duties;

- To express or imply sponsorship or endorsement by the County, except as approved by designated County department management; or
- For personal purpose where activities are for personal enjoyment, private gain or advantage, or an outside endeavor not related to County business purpose. Personal purpose does not include the incidental and minimal use of County IT resources, such as internet usage, for personal purposes, including an occasional use of the internet.

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 access and 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~~electronic communications (e.g., email, text messages, etc.), and data access. Access to County IT resources is a privilege, which access may be modified or revoked at any time, without notice or consent.

Monitoring the access to, and use of County IT resources by County IT users must be approved in accordance with applicable policies and laws on investigations. If any evidence of violation of this policy is identified, the Auditor-Controller's Office of County Investigations must be notified immediately.

~~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.~~

Access Control

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

Access control mechanisms shall be in place to protect against unauthorized access, use, exposure, 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 information.

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

County 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 system 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 Department management.

County IT 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 and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, SecurID cards/tokens, biometric logons, and smartcards).

Fixed passwords or single-factor, ~~which are authentication, which is~~ used for most access authorization, shall be changed at ~~least a~~ minimum of every ninety (90) days.

Two-factor authentication is required for remote access and system administrator (e.g., servers) access to critical servers (e.g., applications) where personal information, confidential information, or otherwise sensitive (e.g., legislative data) information exists unless otherwise stated in County IT security technical and operational standards issued by ISSC.

Information Integrity

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

Accessing County IT Resources Remotely

Remote access to County IT resources by a County IT user shall require approval by designated ~~County~~ Department 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:

- Inclusion of this ~~This~~ Board of Supervisors Policy No. 6.101;
- Board of Supervisors Policy No. 6.102 – Countywide Antivirus Security Policy;
- Board of Supervisors Policy No. 6.104 – Use of Electronic Communications ~~Mail~~ (email) by County Employees;

- Board of Supervisors Policy No. 6.105 – Internet Usage Policy;
- Board of Supervisors Policy No. 6.106 – Physical Security;
- Board of Supervisors Policy No. 6.109 – Security Incident Reporting; and
- Board of Supervisors Policy No. 6.110 – Protection of Information on Portable Computing Devices.

Without limiting the foregoing, County IT users who are authorized to remotely access County IT resources using personally owned computing devices shall ensure that 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.

~~, 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.~~

Privacy

Except as expressly authorized by Board of Supervisors Policy No. 6.105 – Internet Usage, information that is accessed using County IT resources shall be used only for business purposes that have been approved by designated County Department management. Such information County management approved business purposes only and shall not be exposed and/or disclosed to unauthorized individuals.~~others.~~

Confidentiality

Unless specifically authorized by designated County Department management ~~or policy,~~ sending, disseminating, or otherwise exposing and/or disclosing personal information, confidential information, and/or other County IT resources (e.g., software code; business data, documentation, and other information) ~~confidential information or personal information,~~ is strictly prohibited. This includes, without limitation, information that is ~~protected subject to under~~ HIPAA, the 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 both civil and criminal penalties.

Policy Exceptions

Requests for exceptions to this Board of Supervisors (Board) policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approval by the Board. 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 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

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:

**COUNTY OF LOS ANGELES
AGREEMENT FOR ACCEPTABLE USE
AND
CONFIDENTIALITY OF
COUNTY INFORMATION TECHNOLOGY RESOURCES**

ANNUAL

As a County of Los Angeles (County) employee, contractor, subcontractor, volunteer, or other authorized user of County information technology (IT) resources, I understand that I occupy a position of trust. I shall use County IT resources only for County management approved business purposes approved by designated County Department management, except as expressly authorized by Board of Supervisors Policy No. 6.105 – Internet Usage. I only and shall maintain the confidentiality of County IT resources (e.g., business information, personal information, and confidential information).

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 Section 502(c) – Comprehensive Computer Data Access and Fraud Act (set forth, in part, below). I shall immediately report to my management any suspected misuse or crimes relating to County IT resources or otherwise.
2. No Expectation of Privacy: 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 understand that having no expectation to any right to privacy includes, for example, that my access and use of County IT resources may be monitored or investigated by authorized persons at any time, without notice or consent.
3. Activities related to County IT resources: I understand that my activities related to County IT resources (e.g., email, instant messaging, blogs, electronic files, County Internet services, and County systems) may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall not either intentionally, or

through negligence, damage, interfere with the operation of County IT resources. I shall neither, ~~or prevent authorized access to, nor enable unauthorized access to County IT resources and shall use~~ County IT resources responsibly, professionally, ethically, and lawfully.

2.4. 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.

3.5. Security access controls: I shall 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. I shall 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).

4.6. 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.

5.7. ~~Approved b~~Business purposes: Except as expressly provided by Board of Supervisors Policy No. 6.105 – Internet Usage, I shall use County IT resources only for ~~County management approved~~ business purposes approved by designated County ~~d~~Department management 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 designated County ~~d~~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.

8. Remote access: I understand that remote access to County IT resources shall require approval by designated County ~~d~~Department ~~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:

- Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources;
- Board of Supervisors Policy No. 6.102 – Countywide Antivirus Security Policy;

- Board of Supervisors Policy No. 6.104 – ~~Use of Electronic Mail (email) by County Employee Communications;~~
- Board of Supervisors Policy No. 6.105 – Internet Usage Policy;
- Board of Supervisors Policy No. 6.106 – Physical Security;
- Board of Supervisors Policy No. 6.109 – Security Incident Reporting; and
- Board of Supervisors Policy No. 6.110 – Protection of Information on Portable Computing Devices; ~~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.~~

7.9. Confidentiality: I shall not ~~access, store, or send, disseminate, or otherwise expose or disclose to any person or organization, any personal information, confidential information, and/or other 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. This includes, without limitation information that is subject to Health Insurance Portability and Accountability Act of 1996, Health Information Technology for Economic and Clinical Health Act of 2009, or any other confidentiality or privacy legislation.~~

8.10. Computer virus and other malicious devices: I shall not intentionally introduce any malicious device (e.g., computer virus, spyware, worm, ~~key logger, or and~~ malicious code), into any County IT resources. 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 not disable, modify, or delete computer security software (e.g., antivirus software, antispyware 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.

9.11. Offensive materials: I shall not access, create, or distribute (e.g., via email) 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~~ authorized to do so as a part 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.

10.12. Internet: I understand that the Internet is public and uncensored and contains many sites that may be considered offensive in both text and images. Except as expressly authorized by Board of Supervisors Policy No. 6.105 – Internet Usage, I shall use County Internet services only for County management approved business purposes that have been approved by designated County Department management only (e.g., as a research tool or for email communication). ~~I understand that my use of the County Internet services may be logged/stored, may be a public record, and are subject to audit and~~

review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall comply with all County Internet use policies, standards, and procedures. 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.

~~11.13.~~ Electronic Communications and other information~~mail and other information~~: I understand that County electronic communications (e.g., email, text messages, etc.) created, sent, and/or stored using County electronic communications systems/applications/services are the property of the County. All such ~~, and other information, in either electronic or other forms,~~ electronic communications may be logged/stored, ~~may be 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, ~~without notice or consent~~. I shall comply with all County electronic communications email use policies, standards, and procedures and use proper business etiquette when communicating over ~~email~~ County electronic communications systems/applications/services.

~~12. 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.~~

~~13.14.~~ Public forums: Unless I am specifically authorized to do so by designated County Department management as a part of my job function, 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) not specifically approved by designated County Department management.

~~14.15.~~ Internet storage sites: I shall not store County information on any Internet storage site without prior written approval by designated County Department management.

~~15.16.~~ Copyrighted and other proprietary materials: I shall not copy or otherwise use any copyrighted or other proprietary County IT resources materials (e.g., licensed software and documentation, and data), except as permitted by the applicable license agreement and approved by designated County Department management. I shall not use County IT resources to infringe on copyrighted material.

~~16.17.~~ 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.

~~17.~~18. Disciplinary action and other actions and penalties for non-compliance: I understand that my non-compliance with any provision of this Agreement may result in disciplinary action and other actions (e.g., 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.

**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) wrongfully control or obtain money, property, or data.
- (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- (3) Knowingly and without permission uses or causes to be used computer services.
- (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
- (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.
- (9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

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



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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 County Department shall provide County-approved real-time virus protection for all County hardware/software environments to mitigate risk to County IT resources.

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

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

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

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 designated County Department 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:

- Board of Supervisors Policy No. 6.101;
- Inclusion of this Board of Supervisors Policy No. 6.102 – Countywide Antivirus Security Policy;
- Board of Supervisors Policy No. 6.104 –Electronic Communications;
- Board of Supervisors Policy No. 6.105 – Internet Usage Policy;
- Board of Supervisors Policy No. 6.106 – Physical Security;
- Board of Supervisors Policy No. 6.109 – Security Incident Reporting; and
- Board of Supervisors Policy No. 6.110 – Protection of Information on Portable Computing Devices.

Without limiting the foregoing, County IT users who are authorized to remotely access County IT resources using personally owned computing devices shall ensure that 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, antispymware 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.

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 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 be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approval by the Board. 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 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

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
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 security threats affecting the confidentiality, integrity, and/or availability of County information technology (IT) resources.

REFERENCE

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

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 shall be led by the Chief Information Security Officer (CISO) and shall consist of representatives from all County Departments. CCERT shall communicate security information, guidelines for notification processes, identify potential security risks, and coordinate responses to thwart, mitigate, or eliminate 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 DISO and has the responsibility for responding to and/or coordinating the response to security threats to County IT resources within 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 security threats to County IT resources.

Each County Department shall develop a notification process, to ensure management notification within the County Department and to the CCERT, in response to County IT security incidents.

The CCERT and DCERTs have the responsibility to take necessary corrective action to remediate County IT security incidents. Such action shall include all necessary steps to preserve evidence in order to facilitate the discovery, investigation, and prosecution of crimes against County IT resources.

Each County Department shall provide CCERT with contact information, including, without limitation, after-hours, for 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 response to security threats to County IT resources and/or the remediation of County IT security incidents.

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

In instances where violation of any law may have occurred, proper notifications shall be made in accordance with County policies. All necessary action shall be taken to preserve evidence and facilitate the administration of justice.

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 shall be reviewed by the CISO and the Chief Information Officer (CIO), and shall require approval by the Board. 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 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

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

To ensure that access and use of all email-County electronic communications (e.g., electronic mail, instant messaging, etc.) using County information technology (IT) resources systems/applications/services are in accordance with County IT resources policies, County IT security policies, County IT security technical and operational standards, and applicable law. This policy also requires that County email-electronic communications systems/applications/services shall be secured to prevent unauthorized access, to prevent unintended loss or malicious destruction of data and other information, and to provide for the integrity and availability of such systems/applications/services.

REFERENCE

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

Board of Supervisors Policy No. 9.015 – County Policy of Equity

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

2009

California Civil Code Section 1798.29

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.

~~Email~~ Electronic communications systems/applications/services (e.g., electronic mail, instant messaging, etc.) are provided as a County IT resource for conducting County business.

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

County IT users cannot expect any right to privacy when using County electronic communications systems/applications/services. Having no expectation to any right to privacy includes, for example, that County IT users' access to, and use of, County electronic communications systems/applications/services may be monitored or investigated by authorized persons at any time, without notice or consent, or produced as a subject to discovery.

All ~~email communications using County IT resources~~ electronic communications created, sent, and/or stored using County electronic communications systems/applications/services are the property of the County. All ~~email~~ such electronic communications using County IT resources may be logged/stored, ~~are~~ may be a public record, and are subject to audit, ~~and~~ review, and discovery including, without limitation, periodic ~~unannounced~~ monitoring and/or investigation, by authorized persons at any time as directed by designated County Department management. ~~County IT users cannot expect a right to privacy when using County email systems/services.~~

Monitoring the access to, and use of County IT resources by County IT users must be approved in accordance with applicable policies and laws on investigations. If any evidence of violation of this policy is identified, the Auditor-Controller's Office of County

Investigations must be notified immediately.

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

County IT users shall use proper business etiquette when communicating over County electronic communications systems/applications/services.

County Departments shall take appropriate steps to protect all County ~~email~~electronic communication systems/applications/services from various types of security threats.

~~County Internet services shall be used for County management approved business purposes only.~~

All ~~email~~electronic communications created, sent, and/or stored using County electronic communications systems/applications/services using County IT resources shall be retained in compliance with applicable Board of Supervisors policies, departmental policies, and legal requirements, but retention shall be minimized to conserve County IT resources and prevent risk of unauthorized exposure and/or disclosure.

Unless specifically authorized by designated 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 use for ~~of~~ email communications (e.g., create, send, store) d, sent, and/or stored using County electronic communications systems/applications/services using County IT resources may be appropriate when communicating externally to the County's network, or required in some instances, to secure the contents of ~~email~~electronic 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 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 be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approval by the Board. 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 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

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
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) security policy for acceptable use of the Internet utilizing County IT resources.

REFERENCE

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

[Board of Supervisors Policy No. 9.015 – County Policy of Equity](#)

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

[California Civil Code Section 1798.29](#)

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.

~~County Internet services are provided as a County IT resource for conducting County business purposes. Any other use must be minimal or incidental and may not be a use which is substantial enough to result in a gain or advantage to the user or a loss to the County for which a monetary value may be estimated. County IT resources, including, without limitation, County Internet services, shall be accessed and used for County management approved business and non-business purposes only.~~ County Internet services, shall be accessed and used for County management approved business and non-business purposes only. ~~when may not be used in compliance with the following criteria, when the access and use:~~

- ~~• For any unlawful purpose;~~
 - ~~• For any purpose detrimental to the County or its interests;~~
 - ~~• For personal financial gain;~~
 - ~~• In any way that Must in no way Do not undermine in any way or interferes with the access to or use of County IT resources for official County purposes;~~
 - ~~• In any way that Must Do not hinders in any way productivity, efficiency, or customer service, or interferes in any way with a County IT user's obligation to performance of their-his/her official job duties; or in a timely manner~~
 - ~~• To Neither expresses nor implies sponsorship or endorsement by the County, except as approved by designated County department management; or;~~
 - ~~• For personal purpose where activities are for personal enjoyment, private benefit gain or advantage, or an outside endeavor not related to County business purpose. Personal purpose does not include the incidental and minimal use of County IT resources, such as occasional internet usage, for personal purposes, including an occasional use of the internet.. 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 Do not constitute any other access, use, or other activity purpose prohibited by this Board Policy 6.105 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 exposing and/or disclosing any non-public County IT resources information or intellectual property (e.g., software program code; business data, documentation; and or other information; personal data, documentation and or other related information; and any confidential, legislative, or privileged or sensitive data, documentation, and other information) ~~confidential information or personal~~

information, is ~~strictly prohibited~~ in accordance with Board of Supervisors Policy No. 3.040 (see Reference section). This includes, without limitation, information ~~that is~~ protected from disclosure under HIPAA, the HITECH Act, or any applicable information ~~other confidentiality or privacy~~ policy or legislation.~~aw.~~

~~NE~~Except as expressly authorized below in this Board of Supervisors Policy No. 6.105, no County IT user shall access or 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) not specifically approved by designated County Department management.

County Departments may adopt and implement departmental policies and procedures for authorizing one or more specified individuals, as a part of each such individual's assigned job function, to 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) information on behalf of the County Department that is not specifically approved by designated County Department management. Such departmental policies and procedures shall, at a minimum:~~m;~~

- a) ~~(a)~~ Require all information created, exchanged, published, or distributed otherwise to be in compliance with all applicable aspects of 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;
- b) ~~(b)~~ Require the County Department to designate management to regularly monitor the information created, exchanged, published, or distributed in public forums by the specified individual(s); and
- (c) Require the County Department as quickly as practicable to address instances in which the specified individual(s) do not comply with the departmental policies and procedures.

No County IT user shall store County information on any Internet storage site without prior written approval by designated County Department management.

No ~~County IT~~ ~~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.

County IT users must obtain designated County Department management approval to ~~Use access to~~ County Internet services ~~shall require approval by County management.~~ ~~County IT us~~ Authorized users ~~authorized to access County Internet services shall~~ must

not share their credentials, usernames, passwords, or allow another person to access County Internet services using their account.

Access to County Internet services is provided, as needed, to a person at the discretion of each County Department. Access to County Internet services is a privilege, which access may and access may be modified or revoked at any time, without notice or consent by designated County Department management.

County IT users cannot expect any right to privacy when using County Internet services. Having no expectation to any right to privacy includes, for example, that County IT users' access to, and use of, County Internet services may be monitored or investigated by authorized persons at any time, without notice or consent.

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 email sites, chat groups and newsgroups, reviewing materials data 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 must be approved by management, and conducted in accordance with applicable policies and laws on investigations. If any evidence of violation of this policy abuse is identified, notice shall be provided by County Department management to the Auditor-Controller's Office of County Investigations must be notified immediately.

~~The access or 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 are examples of inappropriate access or use of County IT resources, including without limitation County Internet services. This is not a comprehensive list of all possible violations are examples only and are not intended to limit the scope of potential access/use violations:

- Downloading, accessing, storing, displaying or distributing software, unless unless approved by designated County Department County management
- Downloading, accessing, storing, displaying, viewing or distributing material (e.g., movies, music, software, and books) in violation of copyright laws (e.g., movies, music, software, and books)
- Downloading, accessing, storing, displaying, viewing or distributing pornography or other sexually explicit materials
- ~~Any activities that could be construed as a violation of law~~
- Posting or transmitting Soliciting participation in, or advertising scams (e.g., spamming, pyramid schemes, and "make-money-fast" schemes) to others

- Posting or transmitting ~~any message or material which is~~ libelous, ~~or~~ defamatory, fraudulent, or confidential information
- Running/Operating a private business or web site
- Posting or transmitting to unauthorized persons any material deemed to be confidential, ~~information or~~ personal, or otherwise protected from disclosure 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~~ circumvent County security measures, ~~or~~ security measures taken by others connected to the Internet, regardless of whether or not such ~~intrusion attempts are successful or~~ results in corruption or loss of data or other information (e.g., password stealing, phishing, or whaling.
- Knowingly or carelessly distributing malicious code to or from County IT resources
- Accessing, creating, or distributing (e.g., via email) 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 authorized to do so as a part of such County IT user's assigned job function (e.g., law enforcement).

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 be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approval by the Board. 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 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

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Reissue Date:

Sunset Date: July 13, 2008

Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

To establish a County information technology (IT) security policy to ensure that County IT 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 – 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 resources. The plan shall

describe ways in which all County IT resources shall be protected from, without limitation, physical tampering, damage, theft, or unauthorized physical access.

Proper Identification

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

Access to Restricted IT Areas

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

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 both civil and criminal penalties.

Policy Exceptions

Requests for exceptions to this Board of Supervisors (Board) policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approval by the Board. 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 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

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
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) risk assessments of County Departments for the purpose of identifying security threats to, and security vulnerabilities within, County IT resources and initiating appropriate remediation.

REFERENCE

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

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 risk assessments are mandatory and encompass information gathering, analysis,

and determination of security vulnerabilities within the County IT resources, including, without limitation, hardware and software environments, and IT business practices.

IT risk assessments are necessary to analyze and mitigate security threats to the County IT resources, 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 risk assessments shall be conducted on all County IT resources, including, without limitation, applications, servers, networks, and any process or procedure by which the County IT resources are utilized and maintained. IT risk assessments shall also be performed on each facility that houses County IT resources.

An IT risk assessment program (e.g., vulnerability scans of networks, systems, and applications that identifies risks) shall include, without limitation, an inventory of County IT resources; review of County IT resources policies, standards, and procedures; review of County IT security policies, standards, and procedures; assessments and prioritization of 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.

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 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 be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approval by the Board. 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 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

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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 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

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.

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 shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approval by the Board. 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 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

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Reissue Date:

Sunset Date: July 13, 2008

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

[California Civil Code Section 1798.29](#)

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 IT security incidents shall 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 upon discovery to minimize the risk to the County, its employees and assets, and other persons/entities, and to ensure compliance with applicable laws, and to facilitate the prosecution of criminal acts against County IT resources.

The County Department that receives a report of a County IT security incident shall coordinate the information gathering and documenting process and collaborate with other affected County Departments to identify and implement a resolution or mitigation action (e.g., notification of unauthorized access, use, exposure, disclosure, and modification~~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.

Each County Department shall coordinate with one or both of the designated County offices (Chief Information Office and the Auditor-Controller), as applicable, when a County IT security incident occurs. For purposes of this coordination, the CISO has the responsibility for the Chief Information Office. The Chief HIPAA Privacy Officer 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 County IT security incidents that may result in the disruption of business continuity or actual or suspected loss or use, exposure, disclosure, and modification~~disclosure~~ of personal information and/or confidential information shall be reported to the applicable Departmental Information Security Officer (DISO) who shall report to the CISO.

Examples of these incidents include:

- Virus or worm outbreaks that infect ~~at least fifty (50)~~ computing devices, or appear to be crafted to target ~~ed~~ an individual user(s), department(s), resource or data;
- Malicious attacks on telecommunications;
- Web page defacements;
- Actual or suspected loss or use, exposure, disclosure, and modification ~~disclosure~~ of personal information and/or confidential information;
- Lost or stolen computing devices containing personal information and/or confidential information;
- Denial of Service or Distributed Denial of Service attacks;
- Malicious use of web-based applications;
- Unauthorized privilege escalation use of administrator credentials.

Chief HIPAA Privacy Officer

All County IT security incidents that ~~may~~ involve ~~patient p~~ Protected H~~h~~ health i~~n~~formation (PHI) shall be reported by the affected County Departments to the Chief HIPAA Privacy Officer. These incidents may be reported using an on-line form found at www.lacountyfraud.org. Examples of these incidents include:

- Compromise of patient information
- Actual or suspected loss or use, exposure, disclosure, and modification ~~disclosure~~ of patient information

Office of County Investigations (OCI)

All County IT security incidents that may involve non-compliance with any Acceptable Use Agreement (refer to Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources) or the actual or suspected loss or use, exposure, disclosure, and modification ~~disclosure~~ of personal information and/or confidential information shall 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 access and;
- Inappropriate non-work related information which may include, without limitation, ~~pornography,~~ music, and videos to an extent that is not permitted by ~~in accordance with~~ Board of Supervisors Policy No. 6.105 and ~~pornography;~~
- Actual or suspected loss or use, exposure, disclosure, and modification ~~disclosure~~ of personal information and/or confidential information;
- Lost or stolen computing devices containing personal information and/or confidential information.

Chief Information Officer (CIO)

All County IT 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 be reported by the CIO to the Board. 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 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, loss of productivity (where applicable), impact due to the actual or suspected loss or use, exposure, disclosure, and modification disclosure of personal information and/or confidential information, and final actions taken to mitigate and prevent future occurrences of similar incidents.

Actual or suspected loss or use, exposure, disclosure, and modification disclosure of personal information and/or confidential information shall 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 types of personal information and/or confidential information lost or disclosed, and recommended actions to be taken by the persons/entities to mitigate the potential misuse of their information, and any other information required by applicable laws. The timing and content of the notification letter shall be determined in consultation with the CISO.

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 “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.

As used in this policy, the term “Protected Health Information” has the meaning given in 45 CFR §160.103.

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 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:



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 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](#)

[California Civil Code Section 1798.29](#)

-

~~[Authorization to Place Personal Information and/or Confidential Information on a Portable Computing Device \(Authorization\), attached](#)~~

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.

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.

Placing Personal Information and/or Confidential Information On Portable Computing Devices

The County prohibits the unnecessary placement (whether by download or, input, or other means) of personal information and/or confidential information on portable computing devices. However, Designated County Department management may authorize specific County IT users to place personal and/or confidential information on portable computing devices if such County IT users must do so as a part of such County IT users' assigned job functions. Prior to authorizing placement on portable computing devices, such County IT users shall who in the course of County business shall 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 is/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 shall/must be encrypted.

If an A County IT user employee who intends to places personal information and/or confidential information on use any their portable personally procured computing device not owned or provided by the County when used for County business to access and/or store County IT resources, is required to obtain prior written approval from designated County Department departmental management approval that includes, minimally, the Departmental Information Security Officer (DISO). The County IT user shall comply with, and the portable computing device shall comply with, all applicable County IT resources policies, ~~standards~~ standards, and procedures, including, without limitation:

- Board of Supervisors Policy No. 6.101;
- Board of Supervisors Policy No. 6.102 – Countywide Antivirus Security Policy;

- Board of Supervisors Policy No. 6.106 – Physical Security;
- Board of Supervisors Policy No. 6.109 – Security Incident Reporting;
- Inclusion of this Board of Supervisors Policy No. 6.110 – Protection of Information on Portable Computing Devices; and
- Board Policy No. 6.112 – Secure Disposition of Computing Devices.

~~Employee personally procured computing device(s) must adhere to the ISSC approved security and privacy requirements for protection of personal information and/or confidential information when used for County business. Additionally, an Authorization, signed by a designated member of County Department management, shall provide written approval for the particular personal information and/or confidential information to be placed on a portable computing device. The recipient (person using the portable computing device) shall also sign the Authorization to indicate acceptance of the personal information and/or confidential information and to acknowledge his/her understanding of his/her responsibility to protect the information. The Authorization shall be reviewed and renewed, at a minimum, annually. The County Department shall ensure that, in the event the portable computing device is lost or stolen, 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.~~

-

A)B) Protection Requirements for Stored Information Encryption on Portable Computing Devices

~~Security measures shall be employed by all County Departments to~~must safeguard all personal information and/or confidential information on all portable computing devices.

~~All County-owned or provided portable computers shall at all times have automatic full disk, -volume, or file/folder disk 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 ~~is~~ is/are placed/stored on any portable computing device other than a portable computer, all such information shall be encrypted, unless not if feasible and compensating controls that have been approved by the DISO are implemented.

~~The~~Each County Department shall ensure that, in the event ~~the~~ a 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 in accordance with Board of Supervisors Policy .

B)C) Personal Information and/or Confidential 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~~ shall be taken to minimize the amount of information stored on the device required. Additionally, if feasible, such information shall be abbreviated or redacted to limit exposure (e.g., last 4 digits of a Social Security number).

G)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 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 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:



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 County information technology (IT) users.

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. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information

[Board of Supervisors Policy No. 9.015 – County Policy of Equity](#)

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.

~~The Chief Information Office shall facilitate and coordinate with~~ County Departments ~~to~~ shall work with the Chief Information Office to establish and maintain a departmental

~~countywide~~ information security awareness training program.

Information security programs at County Departments shall include, without limitation, information security awareness training that is based on the County Department's information technology use and security IT Use and Security Ppolicies and 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 be provided to all County IT users and should be documented to assist County Department management in determining user awareness and participation. County IT users shall be aware of basic information security requirements and their responsibility to protect all information (personal information, confidential information, other).

Each County Department shall ensure that its County IT users participate in the departmental 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.

Information security awareness training shall be provided to County IT 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 be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approval by the Board. 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 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

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007

Reissue Date:

Sunset Review Date: May 8, 2011

Sunset Review Date:



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

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 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 information 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 information and confidential information.

When using a certified vendor service to render computing devices unreadable and/or unrecoverable, departments must ensure the vendor's contract clearly identifies a County authorized sanitization method and that the department obtains a certificate attesting to wiping the data in accordance with this policy.

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 exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: October 23, 2007

Reissue Date:

Sunset Review Date: October 23, 2011

Sunset Review Date: