County of Los Angeles
CHIEF EXECUTIVE OFFICE
OPERATIONS CLUSTER

WILLIAM T FUJIOKA
Chief Executive Officer

DATE: September 12, 2013
TIME: 1:00 p.m.
LOCATION: Kenneth Hahn Hall of Administration, Room 830

AGENDA

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

1. Call to order – Santos H. Kreimann

A) **Board Letter – COUNTYWIDE CLASS ACTIONS GENERAL RECLASS AND UTILIZATION REVIEW NURSE STAFFING MODEL PHASE II**
CEO Class/Comp – Paul Coyne or designee

B) **Board Letter – COUNTYWIDE CLASS ACTIONS GENERAL RECLASS INFORMATION TECHNOLOGY PHASE II**
CEO Class/Comp – Paul Coyne or designee

C) **Board Letter – REQUEST TO APPROVE A SOLE SOURCE PURCHASE ORDER TO PAY SAS INC. TO PROVIDE TECHNICAL SERVICES FOR THE ADVANCED ANALYTICS DATA MINING PILOT PROJECT**
DCFS/CIO – Philip L. Browning and Richard Sanchez or designee(s)

D) **Board Letter – RECOMMENDATION TO APPROVE AMENDMENT NO. 3 TO EXTEND AGREEMENT NO. 75985 WITH WAUSAU FINANCIAL SYSTEMS, INC. FOR REMITTANCE PROCESSING AND DOCUMENT MANAGEMENT SYSTEM MAINTENANCE AND SUPPORT**
TTC – Mark Saladino or designee

E) **Board Letter – REQUEST APPROVAL OF SECOND AMENDMENT TO PLANNING FUNDING AGREEMENT WITH NEXTEL OPERATIONS, INC. TO RE-BAND AND UPGRADE THE COUNTYWIDE INTEGRATED RADIO SYSTEM**
ISD – Jim Jones or designee

CONTINUED ON PAGE 2

F) **Review of IT Board Policies No. 6.100 through 6.112**
CIO – Richard Sanchez or designee

2. Public Comment

3. Adjournment

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

DRAFT 4

October 1, 2013

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

Dear Supervisors:

COUNTYWIDE CLASSIFICATION ACTIONS
(ALL DISTRICTS - 3 VOTES)

SUBJECT

This letter and accompanying ordinance will update the tables of classes of positions and the departmental staffing provisions by reclassifying positions in various County departments.

IT IS RECOMMENDED THAT THE BOARD:

Approve the accompanying ordinance amending Title 6, Salaries, of the County Code to reclassify 31 ordinanced positions to implement results of classification studies in the Departments of Coroner, Internal Services, Health Services, Mental Health, Public Health, Public Works, and Registrar-Recorder/County Clerk.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The Board of Supervisors (Board) has requested submission of classification letters on a periodic basis throughout the year to facilitate consideration of classification and compensation recommended actions in a timely manner. Approval of these recommendations will provide the ordinance authority for County departments to implement the classification and compensation recommendations in this letter.

These recommendations will ensure the proper classification and compensation of positions based upon the duties and responsibilities assigned to these jobs as performed by the incumbents (Attachments A and B). This is a primary goal of the County's classification and compensation system. Positions reclassified upward, downward and laterally are consistent with the class concepts of the proposed classifications.

These actions are recommended based upon generally accepted principles of classification and compensation. Furthermore, these actions are important in addressing departmental operational needs, and in maintaining consistency in personnel practices throughout the County. The proper classification and compensation of positions facilitates good business operations, and can reduce the number of costly personnel-related problems.

Implementation of Strategic Plan Goals

Your approval of the accompanying ordinance is consistent with the County Strategic Plan Goal 1 - Operational Effectiveness. Specifically, it will address the Service Excellence and Organizational Effectiveness Strategy to improve the quality of the workforce, to achieve departmental operational efficiencies, and to maintain consistency in personnel practices throughout the County.

Reclassification of Nursing Positions

We are implementing the second phase of the inpatient Utilization Review (UR) staffing model. The second phase of our review includes management, supervisory nursing, and clerical support positions. Specifically, we reviewed 21 positions, eight (8) of which are recommended for reclassification in this letter (Attachment A). This staffing model will create a standardized organizational structure for staff managing or supporting inpatient UR functions department-wide and ensure the provision of a high quality of

DRAFT

care to Medi-Cal beneficiaries while minimizing overutilization of costly acute inpatient care.

Reclassifications

There are 31 ordinanced positions in seven (7) departments being recommended for reclassification (Attachments A and B), of which 30 positions are budgeted. The duties and responsibilities assigned to these positions have changed since the original allocations were made. The positions would be more appropriately classified in the recommended classes.

FISCAL IMPACT/FINANCING

The projected budgeted annual cost for the 30 budgeted positions that will be reclassified is estimated to total $143,831 (all funds). Net County cost is estimated to be $13,124. Of this total, the Utilization Review position costs are estimated to total $35,829 with no net County cost. Cost increases associated with upward reclassification actions and compensation changes will be absorbed within the Board's adopted budget for each 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.

Appropriate consultations have been conducted with the impacted employee organizations regarding the recommended classification actions. The accompanying ordinance implementing amendments to Title 6, Salaries, of the County Code has been approved as to form by County Counsel.

DRAFT 4

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Your approval of these classification recommendations will enhance the operational effectiveness of the departments through the proper classification and compensation of positions.

Respectfully submitted,

WILLIAM T FUJIOKA
Chief Executive Officer

WTF:BC:JA
SJM:AB:ra

Attachments (2)

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

DRAFT 4

ATTACHMENT A

RECOMMENDED RECLASSIFICATIONS FOR UTILIZATION REVIEW NURSING POSITIONS

Department	No of Pos.	Present Classification	No of Pos.	Classification Findings
MetroCare Network - Harbor/UCLA Medical Center	1	Medical Transcriber Typist Item No. 2209A N2MV 68L Represented	1	Senior Clerk Item No. 1140A NMV 66E Represented
	2	Supervising Staff Nurse II Item No. 5339A N21 RN08 Represented	1	Assistant Nursing Director, Administration Item No. 5295A N41 RN17 Non-Represented
			1	Utilization Review Nurse Supervisor I Item No. 5125A N21 RN06 Represented
Rancho Los Amigos National Rehabilitation Center	1	Senior Typist-Clerk Item No. 2216A NMV 67D Represented	1	Senior Clerk Item No. 1140A NMV 66E Represented
	1	Supervising Staff Nurse I Item No. 5338A N21 RN06 Represented	1	Utilization Review Nurse Supervisor I Item No. 5125A N21 RN06 Represented
ValleyCare Network - Olive View/UCLA Medical Center	3	Intermediate Typist-Clerk Item No. 2214A NMV 62K Represented	3	Senior Clerk Item No. 1140A NMV 66E Represented
Total	**8**			

DRAFT 4

ATTACHMENT B

RECOMMENDATIONS FOR POSITION RECLASSIFICATIONS

MEDICAL EXAMINER-CORONER

Number of Positions	Present Classification and Salary	Classification Findings and Salary
1	Account Clerk I Item No. 0577A NMV 62F Represented	Accounting Technician II Item No. 0643A NM 72F Represented

The subject position is currently assigned to Fiscal Services and is primarily responsible for performing a variety of paraprofessional accounting assignments, including the more complex technical work by reviewing, maintaining and controlling financial records and fiscal expenditures. Other responsibilities include performing accounting clerical work in the maintenance of accounting records within a comprehensive established framework of procedures. Although the position does not supervise subordinate staff, the assigned duties and responsibilities are more consistent with the class concept for Accounting Technician II, a class which supervises and performs paraprofessional accounting work in preparing, processing, reconciling and maintaining fiscal records requiring a substantive knowledge of County and general accounting procedures. Therefore, we recommend upward classification to Accounting Technician II.

INTERNAL SERVICES

Number of Positions	Present Classification and Salary	Classification Findings and Salary
1	Custodian Item No. 6774A NM 56D Represented	Intermediate Clerk Item No. 1138A NMV 61L Represented

The subject position is assigned to the Custodial Services District 3 Section and will perform clerical functions such as screening phone calls, filing, arranging and maintaining records, data entry into FOS computer applications, and other general office duties. The classification specification for Custodian is characterized by the performance of routine cleaning, sanitizing, and polishing duties in buildings. In contrast, Intermediate Clerk is a class which performs specialized clerical duties. Since the stated duties are consistent with those performed by Intermediate Clerks allocated throughout the County, we recommend the upward reclassification to Intermediate Clerk.

DRAFT 4

ATTACHMENT B

MENTAL HEALTH

Number of Positions	Present Classification and Salary	Classification Findings And Salary
16	Senior Community Worker I Item No. 8104A NR 63C Represented	11 - Community Worker Item No. 8103A NR 61L Represented 3 - Medical Case Worker II Item No. 9002A NM 78D Represented 2 - Senior Community Worker Item No. 8105A NR 67B Represented

The above subject positions were reviewed to better distinguish work performed by positions allocated to classes in Community Welfare Services Series, specifically Community Worker and Senior Community Worker. As a result, the Senior Community Worker I classification was deemed obsolete and the positions were reclassified to classes more commensurate with the actual work performed. Therefore, we recommend downward and upward reclassifications to Community Worker, Medical Case Worker II, and Senior Community Worker.

DRAFT 4

ATTACHMENT B

PUBLIC HEALTH – PUBLIC HEALTH PROGRAMS

Number of Positions	Present Classification and Salary	Classification Findings And Salary
1	Head Departmental Personnel Technician Item No. 1850A NM 94D Non-Represented	Senior Departmental Employee Relations Representative Item No. 1908A NM 101C Non-Represented
1	Intermediate-Typist Clerk Item No. 2214A NMV 62K Represented	Departmental Personnel Assistant Item No. 1842A NM 69J Represented
1	Senior Typist-Clerk Item No. 2216A NMV 67D Represented	Departmental Personnel Assistant Item No. 1842A NM 69J Represented

The subject Head Departmental Personnel Technician position reports to an Administrative Services Manager III and oversees the Employee Relations Unit. The position supervises four (4) full-time staff and has responsibility for serving as the department's lead representative during contract negotiations, representing the department in arbitration, mediation and Unfair Labor Practice hearings. In addition, it serves as the liaison with the Chief Executive Office Employee Relations Division. The position meets the allocation standards for Senior Departmental Employee Relations Representative, a class which is responsible for leading or administering the employee relations program of a large County department with diverse employee bargaining units and complex employee relations issues. Therefore, we recommend upward reclassification to Senior Departmental Employee Relations Representative.

The subject Intermediate-Typist Clerk position is currently assigned to the Classification and Compensation Unit and reports to an Administrative Services Manager II. Duties include assisting technical staff in reviewing requests for new positions and reorganizations, providing information regarding Civil Service Rules, benefits, and deadlines, maintaining a caseload database, and reviewing monthly certification forms for bonuses. The position meets the allocation criteria for Departmental Personnel Assistant, a class which independently performs clerical personnel work and analyzes personnel problems of limited scope and difficulty. Therefore, we recommend upward reclassification to Departmental Personnel Assistant.

DRAFT 4

PUBLIC HEALTH – PUBLIC HEALTH PROGRAMS (Continued)

The subject Senior Typist-Clerk position is assigned to Recruitment and Examining Unit and reports to an Administrative Services Manager II. Duties include assisting technical staff by processing and analyzing job applications, conducting research on comparable positions, calculating test scores, generating test results and notices, conducting test reviews, developing vacancy transfer notices, creating selection plans, and updating the weekly administrative examination calendar. The duties and responsibilities of the position are consistent with the allocation standards for the Departmental Personnel Assistant indicated in the previous paragraph. Therefore, we recommend upward reclassification to Departmental Personnel Assistant.

PUBLIC WORKS

Number of Positions	Present Classification and Salary	Classification Findings and Salary
1	Departmental Personnel Assistant Item No. 1842A NM 69J Represented	Principal Departmental Personnel Assistant Item No. 1845A NM 86D Non-Represented

The subject position is assigned to Human Resources Division, Personnel Operations Unit, where it is responsible for supervising and training lower-level staff in technical and clerical functions. Duties include reviewing, analyzing and processing Personnel Action Requests as well as reviewing work for accuracy and quality control.

The duties and responsibilities meet the allocation criteria of Principal Departmental Personnel Assistant, a classification which assists in the technical personnel work and supervises the processing and maintenance of a variety of personnel documents and records. Therefore, we recommend the upward reclassification to Principal Departmental Personnel Assistant.

DRAFT 4

ATTACHMENT B

REGISTRAR-RECORDER/COUNTY CLERK

Number of Positions	Present Classification and Salary	Classification Findings and Salary
1	Supervising Administrative Assistant II Item No. 0897A NM 94C Non-Represented	Administrative Services Manager II Item No. 1003A NM 96C Non-Represented

The subject position is assigned to the Administration Bureau, Finance and Management Division, Financial Services Section, Cost Recovery Unit. Responsibilities include providing technical and administrative oversight and direction through subordinate supervisors. Duties include reviewing and approving the departmental Account Code update function to track employees' work assignments on time cards, as well as reviewing and approving the claim process for reimbursement of election-related costs from the State of California.

Based on the duties and scope of supervisory responsibilities, the position meets the allocation criteria for the Administrative Services Manager II classification. By definition, the Administrative Services Manager II classification supervises a unit of analysts responsible for performing a full range of difficult to complex analytical assignments within one or more administrative functional areas and makes recommendations for the solution of problems of organization, budget, systems and procedures. Therefore, we recommend an upward reclassification to Administrative Services Manager II.

DRAFT 4

ANALYSIS

This ordinance amends Title 6 - Salaries, of the Los Angeles County Code by adding, deleting, and/or changing certain classifications and numbers of ordinance positions in the departments of Coroner, Health Services, Internal Services, Mental Health, Public Health, Public Works, and Registrar-Recorder/County Clerk.

JOHN KRATTLI
County Counsel

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

RDB:

DRAFT 2

ORDINANCE NO. _____

An ordinance amending Title 6 - Salaries, of the Los Angeles County Code relating to the addition, deletion, and changing of certain classifications and number of ordinance positions in various departments to implement the findings of classification studies.

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

SECTION 1. Section 6.52.010 (Department of Coroner) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS		TITLE
0577A	~~2~~	1	ACCOUNT CLERK I
0643A	~~2~~	3	ACCOUNTING TECHNICIAN II

SECTION 2. Section 6.77.010 (Department of Public Health – Public health services) is hereby amended to delete the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
~~1850A~~	~~1~~	~~HEAD DEPARTMENTAL PERSONNEL TECH~~

DRAFT 2

SECTION 3. Section 6.77.010 (Department of Public Health – Public health services) is hereby amended to add the following class and number of ordinance positions:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
1908A	1	SENIOR DEPTL EMPLOYEE RELATIONS REP

SECTION 4. 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
1842A	~~4~~	6	DEPARTMENTAL PERSONNEL ASSISTANT
2214A	~~167~~	166	INTERMEDIATE TYPIST-CLERK
2216A	~~47~~	46	SENIOR TYPIST-CLERK

SECTION 5. 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
5295A	~~10~~	11	ASST NURSING DIR,ADMINISTRATION
2209A	~~32~~	31	MEDICAL TRANSCRIBER TYPST

DRAFT 2

1140A	~~34~~	35	SENIOR CLERK
5339A	~~5~~	3	SUPERVISING STAFF NURSE II
5125A	~~1~~	2	UTILIZATION REVIEW NURSE SUPVR I

SECTION 6. 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
1140A	~~18~~	19	SENIOR CLERK
2216A	~~33~~	32	SENIOR TYPIST-CLERK
5338A	~~30~~	29	SUPERVISING STAFF NURSE
5125A	~~1~~	2	UTILIZATION REVIEW NURSE SUPVR I

SECTION 7. 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
2214A	~~303~~	300	INTERMEDIATE TYPIST-CLERK
1140A	~~16~~	19	SENIOR CLERK

DRAFT 2

SECTION 8. Section 6.81.010 (Department of Internal Services) is hereby amended to change the number of ordinance positions for the following classes:

ITEM NO.	NO. OF ORDINANCE POSITIONS		TITLE
6774A	~~104~~	103	CUSTODIAN
1138A	~~4~~	5	INTERMEDIATE CLERK

SECTION 9. 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
8103A	~~192~~	203	COMMUNITY WORKER
9002A	~~203~~	206	MEDICAL CASE WORKER II
8105A	~~23~~	25	SENIOR COMMUNITY WORKER
8104A	~~21~~	5	SENIOR COMMUNITY WORKER I

SECTION 10. 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
1842A	~~5~~	4	DEPARTMENTAL PERSONNEL ASSISTANT
1845A	~~1~~	2	PRIN DEPARTMENTAL PERSONNEL ASST

DRAFT 2

SECTION 11. Section 6.114.010 (Department of Registrar-Recorder/County Clerk) is hereby amended to delete the following class and number of ordinance position:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
~~0897A~~	~~1~~	~~SUPVG ADMINISTRATIVE ASSISTANT II~~

SECTION 12. Section 6.114.010 (Department of Registrar-Recorder/County Clerk) is hereby amended to change the number of ordinance positions for the following class:

ITEM NO.	NO. OF ORDINANCE POSITIONS		TITLE
1003A	~~8~~	9	ADMINISTRATIVE SERVICES MANAGER II

SECTION 13. Pursuant to Government Code Section 25123(f), this ordinance shall take effect immediately upon final passage.

[RECLASSOCT13KPCEO]

.

DRAFT 2

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

October 1, 2013

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

Dear Supervisors:

COUNTYWIDE CLASSIFICATION ACTIONS:
INFORMATION TECHNOLOGY OCCUPATIONAL STUDY
(ALL SUPERVISORIAL DISTRICTS)
(3 VOTES)

SUBJECT

This letter and accompanying ordinance will update the tables of classes of positions and departmental staffing provisions by adding two (2) new classifications and by further implementing the findings of the Countywide Information Technology (IT) Occupational Study.

IT IS RECOMMENDED THAT THE BOARD:

Approve the accompanying ordinance amending Title 6, Salaries, of the County Code to add two (2) new classifications; and to reclassify 104 positions in the Department of Public Social Services and one (1) position in the Department of Regional Planning as part of the ongoing implementation of the Countywide IT Occupational Study.

DRAFT 4

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The Board of Supervisors (Board) has requested submission of classification letters on a periodic basis throughout the year to facilitate consideration of classification and compensation recommendations in a timely manner. Approval of these recommendations will provide the ordinance authority for County departments to implement the classification and compensation recommendations in this letter.

These recommendations will ensure the proper classification and compensation of positions based upon the duties and responsibilities assigned to these jobs (Attachments A and B). This is a primary goal of the County's classification and compensation system. Positions reclassified upward, downward and laterally are consistent with the class concepts of the proposed classifications.

We are recommending these actions based upon generally accepted principles of classification and compensation. Furthermore, these actions are important in addressing departmental operational needs and in maintaining consistency in personnel practices throughout the County. The proper classification and compensation of positions facilitates good business operations and can reduce the number of costly personnel-related problems.

New Classifications

At the request of the Chief Information Office, we are establishing two new information technology (IT) Security related classifications that will aid Departmental IT Security Officers (DCIOs) in the development, delivery, and administration of IT security standards, best practices, architecture, and systems. During the last several years, there has been an increase in the overall responsibilities of DCIOs, which has resulted in assignment of lower-level IT positions to assist in carrying out departmental IT security programs. At the same time, County information systems are constantly under threat of cyber-attacks that necessitate IT security expertise to mitigate existing and emerging vulnerabilities. The lack of IT security-specific classifications has affected efforts to effectively recruit, develop, and maintain IT Security technical expertise in order to address these issues. The establishment of these IT security-specific classifications will provide a clear career path in this industry recognized IT specialty field.

Future reclassification recommendations for existing positions to the proposed new classifications will be presented to your Board on a flow basis as departments determine the optimal IT security structure for their respective organizations.

DRAFT

Countywide Information Technology Occupational Study – Phase II

Phase II of the Countywide IT Occupational Study covers the classification and allocation of supervisory and management IT positions. Previously, your Board has approved the creation of nine IT supervisory and management classifications along with four "principal" level IT classifications that reflect current-day IT practices of public and private sector organizations. As we continue to implement Phase II, lower level IT related positions are reviewed and reclassified and organizational structures are realigned where appropriate.

Department of Public Social Services

We have reviewed 425 positions within the Bureau of Contract and Technical Services of the Department of Public Social Services and are recommending reclassification of 104 positions, as well as the reorganization of various IT functions throughout the bureau. These actions will provide the appropriate position allocation and organization structure which will assist in the recruitment and retention of technically skilled staff and aid in reducing reliance on contract agency personnel.

Department of Regional Planning

We are recommending reclassification of one (1) Senior Application Developer to a Principal Application Developer in the Department of Regional Planning to provide technical skills necessary to meet the department's operational needs.

Implementation of Strategic Plan Goals

The Board's approval of the accompanying ordinance will further the County Strategic Plan Goal 1 - Operational Effectiveness. Specifically, it will address the Service Excellence and Organizational Effectiveness Strategy to improve the quality of the workforce, to achieve departmental operational efficiencies, and to maintain consistency in personnel practices throughout the County. These recommendations are in line with the Human Resources Transformation Strategic Initiative Project, which includes the deletion of specialized classes in an effort to streamline the classification system.

FISCAL IMPACT/FINANCING

The projected budgeted annual cost for the 105 positions that will be reclassified is estimated to total $908,452. Net County cost is estimated to be $98,688. Cost increases associated with the upward reclassification actions will be absorbed within the Board's adopted budget for each affected department. No additional funding is required.

DRAFT 4

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.

Appropriate notifications have been made with the impacted employee organizations regarding the recommended classification actions. 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 classification recommendations will enhance the operational effectiveness of the departments through the proper compensation of positions.

Respectfully submitted,

WILLIAM T FUJIOKA
Chief Executive Officer

WTF:BC:JA
SJM:AB:ra

Attachments (2)

c: Executive Office, Board of Supervisors
County Counsel
Auditor-Controller
Human Resources
Chief Information Office
Department of Public Social Services

DRAFT 4

ATTACHMENT A

CLASSIFICATIONS RECOMMENDED FOR ADDITION TO THE CLASSIFICATION PLAN

Proposed Savings/ Cafeteria Benefit Plan	Item No.	Title	Salary Schedule & Level
Savings/ MegaFlex	2602	Information Technology Security Analyst	NM 97F
Savings/ MegaFlex	2603	Information Technology Security Specialist	NM 103H

DRAFT 4

ATTACHMENT B

INFORMATION TECHNOLOGY POSITIONS
RECOMMENDED RECLASSIFICATIONS

RECOMMENDATIONS FOR POSITION RECLASSIFICATIONS

DEPARTMENT OF PUBLIC SOCIAL SERVICES

No of Pos.	Present Classification	No of Pos.	Classification Findings
1	Administrative Assistant II Item No. 0888A NM 81K Represented	1	Information Technology Aide Item No. 2584A NM 71F Represented
1	Administrative Services Manager I Item No. 1002A NM 93C Non-Represented	1	Senior Information Systems Analyst Item No. 2593A NM 99E Non-Represented
1	Administrative Services Manager II Item No. 1003A NM 96C Non-Represented	1	Senior Information Systems Analyst Item No. 2593A NM 99E Non-Represented
4	Administrative Services Manager III Item No. 1004A NM 106B Non-Represented	3	Information Technology Manager I Item No. 2565A N23 S11 Non-Represented
		1	Information Technology Manager II Item No. 2571A N23 S12 Non-Represented
11	Human Services Administrator I Item No. 8021A NM 93C Non-Represented	6	Administrative Services Manager I Item No. 1002A NM 93C Non-Represented
		1	Information Technology Technical Support Supervisor Item No. 2548A NM 95F Non-Represented
		4	Senior Information Systems Analyst Item No. 2593A NM 99E Non-Represented

DRAFT 4

ATTACHMENT B

INFORMATION TECHNOLOGY POSITIONS
RECOMMENDED RECLASSIFICATIONS

DEPARTMENT OF PUBLIC SOCIAL SERVICES (Continued)

No of Pos.	Present Classification	No of Pos.	Classification Findings
5	Human Services Administrator II Item No. 8022A NM 96C Non-Represented	1	Principal Information Systems Analyst Item No. 2594A NM 103H Non-Represented
		1	Senior Application Developer Item No. 2525A NM 97B Represented
		3	Senior Information Systems Analyst Item No. 2593A NM 99E Non-Represented
1	Human Services Administrator III Item No. 8023A NM 106B Non-Represented	1	Information Technology Specialist I Item No. 2569A NM 109H Non-Represented
6	Information Systems Analyst I Item No. 2590A NM 89F Represented	6	Information Systems Analyst II Item No. 2591A NM 92B Represented
6	Information Systems Analyst II Item No. 2591A NM 92B Represented	2	Application Developer II Item No. 2521A N2M 92C Represented
		1	Senior Application Developer Item No. 2525A NM 97B Represented
		2	Senior Information Systems Analyst Item No. 2593A NM 99E Non-Represented
		1	Senior Information Technology Technical Support Analyst Item No. 2547A NM 91F Represented

DRAFT 4

ATTACHMENT B

INFORMATION TECHNOLOGY POSITIONS
RECOMMENDED RECLASSIFICATIONS

DEPARTMENT OF PUBLIC SOCIAL SERVICES (Continued)

No of Pos.	Present Classification	No of Pos.	Classification Findings
33	Information Systems Supervisor I Item No. 2595A NM 99E Non-Represented	4	Information Technology Manager I Item No. 2565A N23 S11 Non-Represented
		1	Information Technology Technical Support Supervisor Item No. 2548A NM 95F Non-Represented
		11	Principal Information Systems Analyst Item No. 2594A NM 103H Non-Represented
		4	Principal Network Systems Administrator Item No. 2561A NM 103H Non-Represented
		1	Senior Application Developer Item No. 2525A NM 97B Represented
		12	Senior Information Systems Analyst Item No. 2593A NM 99E Non-Represented
4	Information Systems Supervisor II Item No. 2596A NM 104B Non-Represented	1	Information Technology Manager I Item No. 2565A N23 S11 Non-Represented
		3	Information Technology Specialist I Item No. 2569A NM 109H Non-Represented

DRAFT 4

ATTACHMENT B

INFORMATION TECHNOLOGY POSITIONS
RECOMMENDED RECLASSIFICATIONS

DEPARTMENT OF PUBLIC SOCIAL SERVICES (Continued)

No of Pos.	Present Classification	No of Pos.	Classification Findings
3	Information Systems Supervisor III Item No. 2597A NM 106J Non-Represented	1 1 1	Information Technology Manager I Item No. 2565A N23 S11 Non-Represented Information Technology Manager II Item No. 2571A N23 S12 Non-Represented Principal Information Systems Analyst Item No. 2594A NM 103H Non-Represented
1	Information Technology Supervisor Item No. 2598A NM 104H Non-Represented	1	Principal Network Systems Administrator Item No. 2561A NM 103H Non-Represented
8	Information Technology Technical Support Analyst I Item No. 2545A NM 83F Represented	5 3	Information Technology Technical Support Analyst II Item No. 2546A NM 87F Represented Network Systems Administrator II Item No. 2559A NM 93F Represented
1	Intermediate Typist-Clerk Item No. 2214A NMV 62K Represented	1	Information Technology Aide Item No. 2584A NM 71F Represented
1	Principal Application Developer Item No. 2526A NM 103E Non-Represented	1	Database Administrator Item No. 2620A NM 104H Non-Represented
1	Program Assistant, PSS Item No. 7980A NM 81B Represented	1	Information Systems Analyst II Item No. 2591A NM 92B Represented

DRAFT 4

ATTACHMENT B

INFORMATION TECHNOLOGY POSITIONS
RECOMMENDED RECLASSIFICATIONS

DEPARTMENT OF PUBLIC SOCIAL SERVICES (Continued)

No of Pos.	Present Classification	No of Pos.	Classification Findings
5	Programming Supervisor II Item No. 2530A NM 103E Non-Represented	1	Database Administrator Item No 2620A NM 104H Non-Represented
		1	Information Technology Manager I Item No. 2565A N23 S11 Non-Represented
		3	Principal Application Developer Item No. 2526A NM 103E Non-Represented
6	Senior Information Systems Analyst Item No. 2593A NM 99E Non-Represented	1	Database Administrator Item No. 2620A NM 104H Non-Represented
		1	Information Technology Supervisor Item No. 2598A NM 104H Non-Represented
		1	Principal Network Systems Administrator Item No. 2561A NM 103H Non-Represented
		3	Senior Network Systems Administrator Item No. 2560A NM 97F Represented

DRAFT 4

DEPARTMENT OF PUBLIC SOCIAL SERVICES (Continued)

No of Pos.	Present Classification	No of Pos.	Classification Findings
1	Senior Information Systems Support Analyst Item No. 2536A NM 97E Non-Represented	1	Senior Information Systems Analyst Item No. 2593A NM 99E Non-Represented
4	Senior Information Technology Technical Support Analyst Item No. 2547A NM 91F Represented	2	Information Systems Analyst II Item No. 2591A NM 92B Represented
		1	Information Technology Technical Support Supervisor Item No. 2548A NM 95F Non-Represented
		1	Network Systems Administrator II Item No. 2559A NM 93F Represented

We are continuing with a phased approach as we implement findings of the Countywide IT Occupational Study, Phase II. In restructuring these IT functions, we are establishing appropriate organization structures and making individual position allocations to facilitate the integration of IT work throughout the County. These recommended classifications provide the appropriate knowledge, skills and abilities for the responsibilities assigned to the subject positions and will aid in the recruitment and retention of staff.

Specifically, we reviewed 425 IT positions within the Bureau of Contract and Technical Services, of which 104 are being recommended for reclassification in this letter. The remaining 321 positions were deemed appropriately classified and require no change. Out of the 104 positions, 71 are in classifications that are either slated for deletion during the implementation of Phase II, or they are in administrative and management classifications that do not provide the technical knowledge, skills and abilities required for the assigned work.

DEPARTMENT OF REGIONAL PLANNING

No of Pos.	Present Classification	No of Pos.	Classification Findings
1	Senior Application Developer Item No. 2525A NM 97B Represented	1	Principal Application Developer Item No. 2526A NM 103E Non-Represented

The subject position reports to the department's Information Technology Manager I and functions as the lead application developer, responsible for leading, developing and performing specialized programming tasks. This position also develops and oversees all database reports and applications, develops policies for database back-up, restoration and installation, and manages the department's key web management systems.

The specific functions being performed are best described by the allocation criteria of the Principal Application Developer, a class that performs highly specialized and complex information systems analysis and programming tasks; acts as technical expert for development or maintenance of one or more major systems; and, may function as a lead for application development projects. Therefore, we recommend an upward reclassification to Principal Application Developer.

ANALYSIS

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

- Adding and establishing the salary for two (2) employee classifications;
- Adding, deleting, and/or changing certain classifications and numbers of ordinance positions in the departments of Public Social Services and Regional Planning.

JOHN KRATTLI
County Counsel

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

RDB:

DRAFT 2

ORDINANCE NO. _____

An ordinance amending Title 6 - Salaries, of the Los Angeles County Code relating to the addition, deletion, and changing of certain classifications and number of ordinance positions in various departments to implement the findings of classification studies.

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 classes:

ITEM NO.	TITLE	EFFECTIVE DATE	SALARY OR SALARY SCHEDULE AND LEVEL	
2602	IT SECURITY ANALYST	_____ *	NM	97F
2603	IT SECURITY SPECIALIST	_____ *	NM	103H

SECTION 2. 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
~~2595A~~	~~33~~	~~INFORMATION SYSTEMS SUPERVISOR I~~
~~2596A~~	~~4~~	~~INFORMATION SYSTEMS SUPERVISOR II~~
~~2597A~~	~~3~~	~~INFORMATION SYSTEMS SUPERVISOR III~~
~~2530A~~	~~5~~	~~PROGRAMMING SUPERVISOR II~~

DRAFT 2

SECTION 3. 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
2620A	3	DATABASE ADMINISTRATOR
2584A	2	INFORMATION TECHNOLOGY AIDE
2565A	10	INFORMATION TECHNOLOGY MANAGER I

SECTION 4. 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
0888A	~~12~~	11	ADMINISTRATIVE ASSISTANT II
1002A	~~98~~	103	ADMINISTRATIVE SERVICES MANAGER I
1003A	~~40~~	39	ADMINISTRATIVE SERVICES MANAGER II
1004A	~~22~~	18	ADMINISTRATIVE SERVICES MANAGER III
2521A	~~10~~	12	APPLICATION DEVELOPER II
8021A	~~302~~	291	HUMAN SERVICES ADMINISTRATOR I
8022A	~~35~~	30	HUMAN SERVICES ADMINISTRATOR II
8023A	~~74~~	73	HUMAN SERVICES ADMINISTRATOR III
2590A	~~11~~	5	INFORMATION SYSTEMS ANALYST I
2591A	~~95~~	98	INFORMATION SYSTEMS ANALYST II

DRAFT 2

2571A	~~5~~	7	INFORMATION TECHNOLOGY MANAGER II
2569A	~~1~~	5	INFORMATION TECHNOLOGY SPECIALIST I
2545A	~~106~~	98	IT TECHNICAL SUPPORT ANALYST I
2546A	~~1~~	6	IT TECHNICAL SUPPORT ANALYST II
2548A	~~8~~	11	IT TECHNICAL SUPPORT SUPERVISOR
2214A	~~2018~~	2017	INTERMEDIATE-TYPIST CLERK
2559A	~~11~~	15	NETWORK SYSTEMS ADMINISTRATOR II
2526A	~~6~~	8	PRINCIPAL APPLICATION DEVELOPER
2594A	~~1~~	14	PRINCIPAL INFO SYSTEMS ANALYST
2561A	~~1~~	7	PRINCIPAL NETWORK SYSTEMS ADMIN
7980A	~~158~~	157	PROGRAM ASSISTANT,PSS
2525A	~~14~~	17	SENIOR APPLICATION DEVELOPER
2593A	~~18~~	36	SENIOR INFORMATION SYSTEMS ANALYST
2536A	~~2~~	1	SENIOR INFO SYSTEMS SUPPORT ANALYST
2547A	~~13~~	10	SENIOR IT TECHNICAL SUPPORT ANALYST
2560A	~~10~~	13	SR NETWORK SYSTEMS ADMINISTRATOR

SECTION 5. Section 6.112.010 (Department of Regional Planning) is hereby amended to delete the following class and number of ordinance position:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
~~2525A~~	~~1~~	~~SENIOR APPLICATION DEVELOPER~~

DRAFT 2

SECTION 6. Section 6.112.010 (Department of Regional Planning) is hereby amended to add the following class and number of ordinance position:

ITEM NO.	NO. OF ORDINANCE POSITIONS	TITLE
2526A	1	PRINCIPAL APPLICATION DEVELOPER

SECTION 7. Pursuant to Government Code Section 25123(f), this ordinance shall take effect immediately upon final passage.

*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 classifications added to Section 6.28.050 of the County Code.

[ITRECLASSOCT13KPCEO]

DRAFT 2

County of Los Angeles
DEPARTMENT OF CHILDREN AND FAMILY SERVICES

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

PHILIP L. BROWNING
Director

FESIA A. DAVENPORT
Chief Deputy Director

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

October 1, 2013

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

Dear Supervisors:

REQUEST TO APPROVE A SOLE SOURCE PURCHASE ORDER TO PAY SAS INC., TO PROVIDE TECHNICAL SERVICES FOR THE ADVANCED ANALYTICS DATA MINING PILOT PROJECT
(ALL SUPERVISORIAL DISTRICTS) (3 VOTES)

SUBJECT:

The Department of Children and Family Services (DCFS) is requesting your Board's authorization for ISD to purchase technical services from SAS Inc., to pilot the Advanced Analytics Data Mining project to estimate children at risk and to improve child welfare operations within the department.

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

IT IS RECOMMENDED THAT YOUR BOARD:

1. Delegate authority to DCFS Director or his designee to sponsor and pay for technical costs associated with consultation services to pilot the Advanced Analytics Data Mining Project to estimate children at risk.
2. Authorize the Internal Services Department, as the County Purchasing Agent, to procure consultancy services from SAS Inc., at a total cost of $99,000.

Sufficient funding is included in the Department's Fiscal Year (FY) 2013-14 Budget Request.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

As a result of the commitment reported to the Board on March 6, 2012, in the report titled "Progress Report on the Development of More Effective Child Safety and Risk Assessment

Tools Inclusive of Structured Decision Making," DCFS began exploring whether a system existed that technologically imports data elements from existing databases and requires little manual input from social workers, to indicate the probability of future risk to children.

DCFS has been in discussions with SAS, Inc. about applying their data mining and analytical capabilities to build upon Los Angeles County's investment in the Enterprise Linkages Project to create a tool for earlier intervention by measuring, monitoring and analyzing risk data associated with child abuse factors.

DCFS envisions compiling de-identified factors on a sufficient number of previous cases in such a manner as to quantify and identify with some reliability the common factors that merit closer attention. Instead of a single, simple measure or collection of independent indicators at a moment in time, the goal of the project is to apply modern data mining tools and methods to currently-collected data to identify the possibility of serious injury and/or death to children under open DCFS supervision.

The process culminated in a proposal for a risk assessment model pilot, which improves on the Structured Decision Making (SDM) tools in several dimensions:

1) Risk scores would be determined by a model incorporating live County data feeds, not hand-entered values, assuring the most up-to-date and relevant information, and eliminating the potential for overrides.
2) Risk scores would be determined through more advanced analytic methods that account for potential interactions between underlying risk factors. The presence of one factor would modify the importance of another. This is a step beyond SDM's basic additive approach, which could mischaracterize child risk.
3) Model sensitivity (detecting risk) and model specificity (minimizing false positives) would be optimized through the data-driven approach that analyzes the association between historic data and case outcomes, as opposed to an arbitrary reliance on a moment-in-time assessment.
4) A robust data framework would emerge for enhanced future analytic opportunities, such as measuring the impact and quality of previous services and interventions.

The proposed pilot would involve DCFS providing SAS, Inc. with three years of de-identified historical data from the existing data structures. SAS, Inc., would link data across the systems and apply its analytic data mining capabilities to identify when cases merit closer attention. Since the outcomes of the selected cases are known, the pilot will test the reliability of a data-driven approach to compiling a clearer picture of children and their environments.

The four primary data sources for use in the pilot include:
1) Child Welfare Services/Case Management System (CWS/CMS);
2) Structured Decision-Making (SDM);
3) Enterprise Linkages Project (ELP); and
4) Critical Incident/Child Fatality Tracking (CIFT).

Based on a similar concept used in the Department of Public Social Services (DPSS) to identify child care fraud, the assessment tool could be a valuable resource for DCFS. The

exploratory analysis and prototyping from this pilot will serve as the foundation for a fully-functioning, operational production solution.

IMPLEMENTATION OF STRATEGIC PLAN GOALS

The recommended action will provide case management proficiency and organization efficiency in delivering services to the public, and is therefore consistent with the principles of the Countywide Strategic Plan Goal No. 1, Operational Effectiveness and Goal No. 3, Integrated Service Delivery.

FISCAL IMPACT/FINANCING

For the purpose of the pilot, SAS, Inc. will provide all the necessary software, services and hosting support to implement the pilot and set the stage for a production implementation of the Child Welfare and Risk Prevention Solution at no cost to the County. However, SAS, Inc. proposes consultant service fees for the entire pilot, which will include the services of a Managing Consultant, an Expert Consultant, and a Senior Systems Consultant for a total of $99,000. The sole source purchase order will be financed using Net County Cost. Sufficient funding is included in the Department's FY 2013-14 Budget.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

Only data elements and risk factors identified by DCFS will be used. SAS, Inc. and DCFS agreed that only de-identified data would pass from DCFS to SAS, Inc., in order to safeguard confidentiality. SAS, Inc. would draw data from four sources. One of these data sources is CWS/CMS. DCFS managers will notify the California Department of Social Services (CDSS) of the intended use and obtain CDSS' written approval confirming that it is a use consistent with the role of CWS/CMS and federal regulations.

The Enterprise Linkages Project pulls data from many different County department databases, and links them via a unique identifier. The data that is extracted is normally de-identified. The Office of the County Counsel will be notified to review the impacts of the pilot for each affected department.

Board approval of the proposed pilot is required. On June 21, 2011, on a motion by Supervisor Yaroslavsky, the Board of Supervisors delegated administrative oversight authority to the Chief Executive Office for the purpose of coordinating the following data-sharing initiatives that include DCFS and Probation: 1) Enterprise Master Person Index; 2) Enterprise Linkages Project; 3) Homeless Prevention Initiative Cost Avoidance Studies; 4) Linkages; 5) Outcomes of Youth Exiting Dependent Care; 6) Skid Row Collaborative Cost Avoidance Study; and 7) Residential Placement Protocols. The Board further instructed the Chief Executive Office to return to the Board for approval of any future, additional or amended contracts that relate to these ongoing data-sharing initiatives, as well as requests for delegation of administrative oversight for any new data-sharing initiatives.

As such, authorization for ISD to purchase these necessary services is being requested. The offices of the Internal Services Department, Chief Information Officer and the Chief Executive Officer have reviewed and approved this Board Letter.

CONTRACTING PROCESS

The acquisition of consultancy services falls within the authority of the Purchasing Agent. Any such purchases will be requisitioned through, and accomplished by the Purchasing Agent in accordance with the County's purchasing policies and procedures. This is a sole source procurement. Formal bidding requirements of Los Angeles County Code Chapter 2.121 do not apply.

IMPACT ON CURRENT SERVICES

The goal of this pilot project is to apply modern data mining tools and methods to currently-collected data to identify the possibility of serious injury and/or death to children under open DCFS supervision. The project will create a tool to further enhance assessment and intervention by measuring, monitoring and analyzing key risk factors associated with child abuse.

Approval of the proposed consultancy services will allow DCFS to continue to ensure the well-being of children and families in our care.

CONCLUSION

Your Board's approval of the recommendations will also authorize the Internal Services Department, as the County Purchasing Agent, to procure consultancy services required to pilot the Advanced Analytics Data Mining Project. Upon approval by the Board of Supervisors, it is requested that the Executive Office/Clerk of the Board send an adopted copy of this Board Letter to:

1. Department of Children and Family Services
   Business Information Division
   Attention: Cecilia Custodio, Division Chief
   12440 E. Imperial Highway
   Norwalk, CA 90650

2. Internal Services Department
   Purchasing and Contract Services
   Attention: Gerald R. Plummer, Division Manager
   1100 N. Eastern Avenue
   Los Angeles, CA 90063

3. SAS Institute Inc.
   Contracts Administration
   Attention: Victoria Clayton, Senior Manager,
   SAS Campus Drive
   Cary, NC 27513

4. Chief Information Office
   Attention: Richard Sanchez, Chief Information Officer
   493 Kenneth Hahn Hall of Administration
   500 W. Temple St.
   Los Angeles, CA 90012

Respectfully submitted:

PHILIP L. BROWNING
Director

Reviewed by:

RICHARD SANCHEZ
Chief Information Officer

PLB:CC
PD:nc

Enclosures

c: Chief Executive Office
   Chief Information Office
   Executive Officer, Board of Supervisors

DRAFT

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 437
LOS ANGELES, CA 90012
TELEPHONE (213) 974-2101 FAX: (213) 626-1812

HOME PAGE
TTC.LACOUNTY.GOV

PROPERTY TAX PORTAL
LACOUNTYPROPERTYTAX.COM

DRAFT

October 1, 2013

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

Dear Supervisors:

TREASURER AND TAX COLLECTOR:
RECOMMENDATION TO APPROVE AMENDMENT NUMBER THREE TO EXTEND AGREEMENT NUMBER 75985 WITH WAUSAU FINANCIAL SYSTEMS, INC. FOR REMITTANCE PROCESSING AND DOCUMENT MANAGEMENT SYSTEM MAINTENANCE AND SUPPORT
(ALL DISTRICTS - 3 VOTES)

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

SUBJECT

The recommended action is to approve Amendment Number Three to Agreement Number 75985 with Wausau Financial Systems, Inc. (Wausau), (a) to increase the maximum County of Los Angeles (County) obligation under Agreement Number 75985 by $1,758,586 to $5,326,124; (b) to extend the current term of the maintenance, support, and professional services agreement for the Remittance Processing and Document Management System (System); and (c) to provide funding for necessary upgrades to the System.

IT IS RECOMMENDED THAT YOUR BOARD:

1. Approve and instruct the Chairman to sign Amendment Number Three to Agreement Number 75985 with Wausau to extend the Agreement for one year through January 31, 2015, and an additional four optional one-year renewal periods, and to increase the maximum County obligation under the Agreement by $1,758,586 to $5,326,124 to be used (a) to upgrade the System, and (b) to obtain further maintenance, support, and professional services through the one-year extension period.

2. Delegate authority to the Treasurer and Tax Collector (TTC) or his designee to execute amendments to the Agreement that (a) extend the term of the Agreement for each of the four optional one-year renewal periods provided for in the Agreement, and (b) make necessary modifications to the Agreement in connection with each such extension, provided that such amendments do not increase the maximum County obligation under the Agreement by more than $375,000 for each renewal period. In the event a particular renewal period exceeds such maximum allowable amount, the TTC shall request Board approval for any additional funding.

3. Delegate authority to the TTC to negotiate and/or execute amendments to existing escrow agreements for source code and/or replacement escrow agreements for source code and pay fees under such agreements.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The System was implemented in August 2000 and is currently processing five million remittance payments per year, totaling approximately $14 billion, for various accounts receivable applications, including property tax. The System consists of software and hardware purchased from Wausau under predecessor Agreement Number 72748. The software supports the remittance workflow which reads and images stubs and checks and applies technology to read check amounts via Courtesy Amount Recognition, Legal Amount Recognition, and Optical Character Recognition. The System produces daily reports and deposit files for four major banks.

On December 19, 2006, your Board approved sole source successor Agreement Number 75985 (Agreement) with Wausau, extending services for an additional four years, commencing on February 1, 2007, through January 31, 2011, with a three-year extension and increasing the maximum Agreement sum to obtain further maintenance, support, and professional services with respect to the System. The Agreement is set to expire on January 31, 2014.

DRAFT

In planning for the future replacement of the System, the TTC requested the establishment of a designation in the TTC's FY 2008-09 proposed budget. However, the Chief Executive Office denied that request due to the economic downturn and the overall state of the County's budget. Since that time, the TTC's budget has been cut significantly (greater than 30 percent), and the TTC currently lacks the necessary fiscal resources to fund a replacement system that was estimated to cost between $8 million and $10 million. Upgrading versus replacing the System proved to be a successful and cost-effective measure in the past and is again a viable solution.

The TTC utilized all available renewal options under the existing Sole Source Agreement and is seeking a new term extension. Amendment Number Three (Attachment III) extends the term of the Agreement for one year with four optional one-year renewal periods, for a total possible extension of five years through January 31, 2019, and increases the maximum County obligation under the Agreement by $1,758,586 to $5,326,124. The increase will be used (a) $1,231,524 to upgrade the System, (b) $302,062 to obtain further maintenance, support, and professional services for the System for the one-year extension period, and (c) $225,000 to the pool of dollars available under the Agreement for additional services/System components.

The consequences of not continuing to maintain and upgrade the current System are very significant. The depositing of monies would slow, thereby decreasing available cash balances and decreasing interest earnings. The posting of payments to the appropriate accounts receivable systems would also slow, thereby impacting the ability of the TTC and the other departments to respond to constituent inquiries timely. As well, the TTC's comprehensive system of internal controls to prevent theft or misuse of funds would be compromised.

The upgrade to the System will be effectuated through change notices executed by the TTC and approved by the Chief Information Office (CIO) and County Counsel, using delegated authority granted by your Board under the Agreement. The upgrade to the System will provide for replacement of existing software and hardware that will no longer be supported by the manufacturer to ensure that the System is compliant and fully operational through January 31, 2019.

<u>Implementation of Strategic Plan Goals</u>

Implementation of the upgraded System will meet the County's Strategic Plan Goals of Organizational Effectiveness (Goal 1) by providing for an effective Remittance Processing System and Fiscal Sustainability (Goal 2) by leveraging information technology resources to sustain efficient County operations.

DRAFT

FISCAL IMPACT/FINANCING

The maximum amount of Amendment Number Three is $1,758,586 and is included in the TTC's Fiscal Year (FY) 2013-14 Adopted Budget. The funds for the upgrade, $1,231,524 will initially be allocated to the pool of dollars available under the Agreement for additional services/System components. Additionally, $225,000 will be allocated to the pool of dollars to be available for the extension periods for additional services/System components. Maintenance for the first year of the extension is $302,062.

The contractor agrees to extend to the County a two percent multi-year discount for maintenance services.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The CIO concurs with TTC's recommendation. The CIO's analysis is attached as Attachment I.

In accordance with your Board's Policy Number 5.100, Sole Source Contracts, the Sole Source Checklist is attached as Attachment II. The Notice of Intent to negotiate a Sole Source Agreement extension was delivered to your Board on July 30, 2013.

Amendment Number Three (Attachment III) has been reviewed and approved as to form by County Counsel.

The Agreement contains all Board required and legally required provisions.

The Agreement/project is included the TTC's Business Automation Plan for FY 2013-14.

CONTRACTING PROCESS

This is a Sole Source Agreement extension with Wausau, which is the current contractor. The System was implemented in August 2000 after a competitive solicitation, and consists of software that is proprietary to Wausau and hardware that was purchased under the predecessor Agreement Number 72748 from Wausau. Therefore, Wausau is the only contractor that can provide comprehensive maintenance, support, and professional services for this System. Additionally, Wausau is qualified to provide these services due to Wausau's knowledge of the County's business operations and the intricacies of maintaining the System.

DRAFT

A new/replacement System is estimated to cost between $8 million and $10 million. Given budget curtailments to the TTC in excess of 30 percent over the last five years, the Department does not currently have the resources to purchase a new System. Upgrading versus replacing the System proved to be a successful and cost-effective measure in the past and is again a viable solution. In addition, a new contractor(s), unfamiliar with TTC's business operations and requirements, would experience an extensive learning curve, which could negatively impact the TTC's current operation and ability to process payments.

IMPACT ON CURRENT SERVICES

The recommended actions will provide for continuation of the Remittance Processing services that the TTC is currently providing.

The upgrade implementation will take place during off-peak hours between critical processing jobs to mitigate any transition issues and to ensure that the System testing causes minimal or no disruption to the TTC's operations. Implementation of the upgrade to the System will ensure uninterrupted hardware and software maintenance and support services for the System for the term of the Agreement.

CONCLUSION

Instruct the Executive Officer-Clerk of the Board to return two signed originals of Amendment Number Three to Agreement Number 75985 and one adopted stamped Board letter to the TTC.

Respectfully submitted,

MARK J. SALADINO
Treasurer and Tax Collector

Reviewed by:

RICHARD SANCHEZ
Chief Information Officer

MJS:JK:SDP
EVT:MVA:VMA:lc

Attachments (3)

c: Chief Executive Officer
County Counsel
Executive Officer, Board of Supervisors
Auditor-Controller
Chief Information Officer

DRAFT

County of Los Angeles
INTERNAL SERVICES DEPARTMENT
1100 North Eastern Avenue
Los Angeles, California 90063

JIM JONES
Acting Director

Telephone: (323) 267-2101
FAX: (323) 264-7135

"To enrich lives through effective and caring service"

October 8, 2013

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

Dear Supervisors:

REQUEST APPROVAL OF SECOND AMENDMENT TO PLANNING FUNDING AGREEMENT WITH NEXTEL OPERATIONS, INC. TO RE-BAND AND UPGRADE THE COUNTYWIDE INTEGRATED RADIO SYSTEM (CWIRS) (ALL DISTRICTS – 3 VOTES)

SUBJECT

Approval of a second amendment to the Planning Funding Agreement with Nextel Operations, Inc., a wholly owned subsidiary of Sprint Nextel Corporation (Sprint Nextel), to accept additional funds to be paid to the County of Los Angeles (County) by Sprint Nextel in an aggregate amount of $27,801.50 as a true-up for the planning phase of the County's project to re-band and upgrade CWIRS.

IT IS RECOMMENDED THAT YOUR BOARD:

1. Approve and instruct the Chairman to sign the Second Amendment to the Planning Funding Agreement (Attachment I) with Sprint Nextel, which provides an additional $27,801.50 for the planning phase of the County's project to replace and upgrade CWIRS as part of the Federal Communications Commission's (FCC) frequency re-banding mandate.

2. Authorize the Acting Director of Internal Services Department (ISD) to accept $27,801.50 as true-up and close-out funding under the Planning Funding Agreement, including $16,926.50 to be paid to ISD for in-house labor costs, and $10,875 to be paid directly to outside counsel for legal services.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

Background and Phases of the CWIRS project

CWIRS is a County radio system used for mobile communications by a number of departments, including Health Services, Public Works, Probation, Animal Care & Control and ISD. In addition to serving the day-to-day operations of its user departments, CWIRS is the County's primary disaster recovery mobile communications system in a major emergency.

About fifteen years ago, public agencies such as the County using the 800 MHz radio band frequency started to experience radio interference caused by adjacent frequency use by Nextel Communications, Inc. (now Sprint Nextel). To eliminate this interference and allocate frequencies for more efficient use, the FCC issued orders in 2004 requiring all 800 MHz licensees, including the County, to move to new frequencies. The FCC also ordered Sprint Nextel to provide funding to all licensees for such reconfiguration.

Under the FCC order, reconfiguration is a two-phase project. Phase 1 was planning and design. Phase 2 is implementation. Your Board approved the Phase 2 agreements on May 14, 2013, and implementation is currently underway.

Your Board approved the Phase 1 agreements, including the Planning Funding Agreement, on February 20, 2007. Phase 1 has been completed, and the proposed Second Amendment is to true-up and close out Phase 1.

The Second Amendment to the Planning Funding Agreement

Under the FCC procedure for Phase 1 Planning, a true-up process was undertaken by the County and Sprint Nextel to determine the actual amount of funding due from Sprint Nextel to the County. The amount of funding previously approved and accepted by your Board for the Planning Funding Agreement was $442,408.00.

Per the true-up review, the County and Sprint Nextel determined that the total funding to be paid by Sprint Nextel should be $470,209.50, an increase of $27,801.50. This increase is due to the cost of labor for performance of additional work by County staff and outside legal counsel for the planning phase. The increase of $27,801.50 is to be paid by Sprint Nextel and has been approved by both the FCC 800 MHz Transition Administrator and by Sprint Nextel. There is no cost to the County for this amendment.

Implementation of Strategic Plan Goals

The recommended contract amendment supports County Strategic Plan Goal Number 1 for Operational Effectiveness, by providing timely delivery of customer oriented and efficient public services. It will enhance the County radio system for disaster recovery by upgrading its operation to state of the art technology. This recommended action also supports Goal Number 2 for Fiscal Sustainability. The County will be able to upgrade its aged CWIRS radio system without contributing general fund monies.

FISCAL IMPACT/FINANCING

Under the amendment to the Planning Funding Agreement (Attachment I), Sprint Nextel will provide an additional $27,801.50 over the amount of $442,408.00 previously approved by your Board. This will bring the new total to be paid by Sprint Nextel for planning funding to $470,209.50.

The $27,801.50 is itemized as follows:

Labor costs for County staff to be paid to ISD	$16,926.50
Legal services to be paid to the County's outside counsel	$10,875.00
Total	$27,801.50

Under the FCC order and planning funding agreement, County planning costs are fully reimbursed by Sprint Nextel, requiring no net County cost. The County will receive its cost reimbursement portion directly from Sprint Nextel. Sprint Nextel will pay the legal services portion directly to the County's outside counsel, Shulman, Rogers, Gandal, Pordy & Ecker, P.A.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The FCC uses a Transition Administrator (TA) to administer the 800 MHz re-banding process and review re-banding expenditures for compliance with the FCC order. The TA reviewed and approved this proposed second amendment to the Planning Funding Agreement, and has issued an approval letter to the County for the additional funding of $27,801.50.

The recommended second amendment has been reviewed and approved as to form by outside counsel, Jeffrey Rubin of Shulman, Rogers, Gandal, Pordy & Ecker, P.A., as well as County Counsel.

CONTRACTING PROCESS

This proposed Second Amendment is a true-up amendment to a Planning Funding Agreement approved by your Board on February 20, 2007.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

The County is maintaining existing CWIRS radio functionality during the current implementation period and will continue to do so until users are migrated to the upgraded system. All activity is being coordinated with departments to ensure that there is minimal or no impact on operations. There is no employee impact as a result of the planning funding agreement or other re-banding agreements.

CONCLUSION

Approval of this second amendment to the Planning Funding Agreement will close out Phase 1 and accept additional funding of $27,801.50 in true-up.

Respectfully submitted,

JIM JONES
ACTING DIRECTOR, ISD

JJ:JLG:DC:RK
Attachment

c: Chief Executive Officer
County Counsel
Chief Information Officer

800 MHz Transition Administrator

The Official Reconfiguration Manager

August 19, 2013

Mr. William Jenkins
Sprint Nextel
6575 The Corners Parkway
Norcross, GA 30092

RE: PLANNING FUNDING AGREEMENT # DL8910428072 - Amendment 2
INCUMBENT: County of Los Angeles, California
AMOUNT: $27,801.50

Dear Mr. Jenkins:

The 800 MHz Transition Administrator, LLC ("TA") has reviewed this Amendment, submitted to the TA on August 6, 2013. The TA hereby grants its approval of this Planning Funding Agreement amendment in the amount of $27,801.50. The total value of the Planning Funding Agreement has been increased to $470,209.50

In addition, when available please forward a copy of the fully executed Amendment for our records. Note that any changes to the Agreement must be submitted to the TA for review and approval.

Should you have any questions in this matter, please do not hesitate to contact the Transition Administrator at contracts@800ta.org.

Very truly yours,

Jon Strbak
800 MHz Transition Administrator, LLC

cc: Alan Tilles
Ian Telfer, P.E.

SHULMAN ROGERS | GANDAL PORDY ECKER

JEFFREY W. RUBIN | ATTORNEY-AT-LAW
301.231.0931 jrubin@shulmanrogers.com

August 22, 2013

VIA FEDERAL EXPRESS

Ian Telfer, P.E.
IT Specialist
Los Angeles County, ISD
1110 Northern Eastern Avenue
Los Angeles, CA 90063

Re: Second Amendment to Planning Funding Agreement ("Amendment")

Dear Ian:

Enclosed are three (3) originals of the above referenced Amendment requested by Sprint. Please proceed to obtain Board approval of the Amendment and have the County execute as follows:

1. Please have the County sign page 2 of the Amendment.
2. Please have the County sign the Certification on page 9 of the Amendment.
3. Do not date page 7 but do date page 9 of the Amendment.
4. Please return all executed originals to me to be signed by Sprint.

As always, please call me with any questions.

Sincerely yours,

SHULMAN, ROGERS, GANDAL,
PORDY & ECKER, P.A.

By: _____
Jeffrey W. Rubin

Enclosures

cc: Stephen Cohen, Los Angeles County

SECOND AMENDMENT TO PLANNING FUNDING AGREEMENT

THIS SECOND AMENDMENT shall amend and revise that certain Planning Funding Agreement (the "Agreement") executed on April 11, 2007, as amended, by and between the County of Los Angeles, a political subdivision of the State of California ("Incumbent"), and Nextel Operations, Inc., a wholly owned indirect subsidiary of Sprint Nextel Corporation, a Kansas corporation ("Nextel"). Nextel and Incumbent may be referred to collectively in this Agreement as the "Parties."

WHEREAS, the Parties wish to amend certain costs in the Agreement; and

NOW, THEREFORE, the Parties, in accordance with the provisions of Paragraph 5 of the Agreement, hereby agree to amend and revise the Agreement as follows:

1. That the following Internal Labor Table, Schedule B, is hereby deleted:

INTERNAL Labor Table – FREQUENCY ANALYSIS

Planning Cost Category/Tasks	Start Date	End Date	Labor Hours	Labor Rate	Cost (Hrs x Rate)	Expenses	Labor Name
A01: Transmitter Combiner and Receiver Multicoupler Suitability Assessment	ED	ED+42 days	63	108	6804		County Technical Staff
A02: Intermodulation Interference Study		42 days from receipt of FPR	130	108	14040		County Technical Staff
A03: Bidirectional Amplifier Assessment	ED	ED+42 days	20	108	2160		County Technical Staff
Total Internal Cost					$23004	0	

And is replaced with the following:

Category/Tasks	Date	Date	Hours	Rate	(Hrs x Rate)		
A01: Transmitter Combiner and Receiver Multicoupler Suitability Assessment	ED	ED+42 days	63	108	6804		County Technical Staff

A02: Intermodulation Interference Study		42 days from receipt of FPR	130	108	14040		County Technical Staff
A03: Bidirectional Amplifier Assessment	ED	ED+42 days	20	108	2160		County Technical Staff
Amendment - 2							
A01: Transmitter Combiner and Receiver Multicoupler Suitability Assessment	ED	ED+42 days	(63)	108	(6804)		County Technical Staff
A02: Intermodulation Interference Study		42 days from receipt of FPR	(130)	108	(14040)		County Technical Staff
A03: Bidirectional Amplifier Assessment	ED	ED+42 days	(20)	108	(2160)		County Technical Staff
A01: Transmitter Combiner and Receiver Multicoupler Suitability Assessment	ED	ED+42 days	30	115	$3,450		County Technical Staff
A03: Bidirectional Amplifier Assessment	ED	ED+42 days	12	115	$1,380		County Technical Staff
Total Internal Cost					**$4,830**	0	

2. That the following Internal Labor Table, Schedule B, is hereby deleted:

INTERNAL Labor Table – SYSTEM INVENTORY

Planning Cost Category/Tasks	Start Date	End Date	Labor Hours	Labor Rate	Cost (Hrs x Rate)	Expenses	Labor Name
B01: Infrastructure Inventory	ED	ED+42 days	40	108	4320		County Technical Staff
B02: Subscriber Inventory	ED	ED+42 days	140	108	15120	571	County Technical Staff
B03: BDA Inventory	ED	ED+42 days	10	108	1080		County Technical Staff

Total Internal Cost					$20520	571	

And is replaced with the following:

Planning Cost Category/Tasks	Start Date	End Date	Labor Hours	Labor Rate	Cost (Hrs x Rate)	Expenses	Labor Name
B01: Infrastructure Inventory	ED	ED+42 days	40	108	4320		County Technical Staff
B02: Subscriber Inventory	ED	ED+42 days	140	108	15120	571	County Technical Staff
B03: BDA Inventory	ED	ED+42 days	10	108	1080		County Technical Staff
Amendment - 2							
B01: Infrastructure Inventory	ED	ED+42 days	(40)	108	(4320)		County Technical Staff
B02: Subscriber Inventory	ED	ED+42 days	(140)	108	(15120)	(571)	County Technical Staff
B03: BDA Inventory	ED	ED+42 days	(10)	108	(1080)		County Technical Staff
B02: Subscriber Inventory	ED	ED+42 days	9	115	$1,035		County Technical Staff
B03: BDA Inventory	ED	ED+42 days	3	115	$345		County Technical Staff
Total Internal Cost					**$1,380**	**0**	

3. That the following Internal Labor Table, Schedule B, is hereby deleted:

INTERNAL Labor Table – ENGINEERING/IMPLEMENTATION PLAN

Planning Cost Category/Tasks	Start Date	End Date	Labor Hours	Labor Rate	Cost (Hrs x Rate)	Expenses	Labor Name
C01: Continuity of communication Service	ED	ED+59 days	200	108	21600	1141	County Technical Staff
C02: Site Reconfiguration Planning	ED+7 days	ED+73 days	200	108	21600		County Technical Staff

C03: Subscriber Retune/ Reprogram/ Replace Determination	ED	ED+42 days	100	108	10800		County Technical Staff
Total Internal Cost					$54000	1141	

And is replaced with the following:

INTERNAL Labor Table – ENGINEERING/IMPLEMENTATION PLAN

Planning Cost Category/Tasks	Start Date	End Date	Labor Hours	Labor Rate	Cost (Hrs x Rate)	Expenses	Labor Name
C01: Continuity of communication Service	ED	ED+59 days	200	108	21600	1141	County Technical Staff
C02: Site Reconfiguration Planning	ED+7 days	ED+73 days	200	108	21600		County Technical Staff
C03: Subscriber Retune/ Reprogram/ Replace Determination	ED	ED+42 days	100	108	10800		County Technical Staff
Amendment - 2							
C01: Continuity of communication Service	ED	ED+59 days	(200)	108	(21600)	(1141)	County Technical Staff
C02: Site Reconfiguration Planning	ED+7 days	ED+73 days	(200)	108	(21600)		County Technical Staff
C03: Subscriber Retune/ Reprogram/ Replace Determination	ED	ED+42 days	(100)	108	(10800)		County Technical Staff
C01: Continuity of communication Service	ED	ED+59 days	65	115	$7,475		County Technical Staff
C02: Site Reconfiguration Planning	ED+7 days	ED+73 days	208	115	$23,920		County Technical Staff
C03: Subscriber Retune/ Reprogram/ Replace Determination	ED	ED+42 days	26	115	$2,990		County Technical Staff

Total Internal Cost					**$34,385**	**0**	

4. That the following Vendor Labor Table, Schedule B, is hereby deleted:

VENDOR Labor Table – LEGAL PFA

Planning Cost Category/Tasks	Start Date	End Date	Labor Hours	Labor Rate	Cost (Hrs x Rate)	Expenses	Vendor Name
PFA Legal Advice			0		0		Fletcher, Heald & Hildreth
PFA Negotiations*			0		0		Fletcher, Heald & Hildreth
PFA Contract Review	Dec 15 2006	Feb 8 2007	6	370	2220		Fletcher, Heald & Hildreth
Total Vendor Cost					2220		

*Negotiations not applicable for Fast Track

And is replaced with the following:

Planning Cost Category/Tasks	Start Date	End Date	Labor Hours	Labor Rate	Cost (Hrs x Rate)	Expenses	Vendor Name
PFA Legal Advice			0		0		Fletcher, Heald & Hildreth
PFA Negotiations*			0		0		Fletcher, Heald & Hildreth
PFA Contract Review	Dec 15 2006	Feb 8 2007	6	370	2220		Fletcher, Heald & Hildreth
Amendment - 2							
Additional legal fees			25	435	$10,875		SHULMAN, ROGERS, GANDAL, PORDY & ECKER, P.A.
Total Vendor Cost					**$13,095**		

*Negotiations not applicable for Fast Track

5. That the following Internal Labor Table, Schedule B, is hereby deleted:

INTERNAL Labor Table – PROJECT MANAGEMENT

Planning Cost Category/Tasks	Start Date	End Date	Labor Hours	Labor Rate	Cost (Hrs x Rate)	Expenses	Labor Name
E01: Planning Management	ED	ED+77 days	360	115	41400		County Project Manager
E02: FRA Negotiations & Contract Review	ED+77 days	ED+98 days	120	115	13800		County Project Manager
			80	94	7520		County Regulator Affairs
Total Internal Cost					$62720		

*Negotiations support expected to be minimal or not applicable for Fast Track

And is replaced with the following:

INTERNAL Labor Table – PROJECT MANAGEMENT

Planning Cost Category/Tasks	Start Date	End Date	Labor Hours	Labor Rate	Cost (Hrs x Rate)	Expenses	Labor Name
E01: Planning Management	ED	ED+77 days	360	115	41400		County Project Manager
E02: FRA Negotiations & Contract Review	ED+77 days	ED+98 days	120	115	13800		County Project Manager
			80	94	7520		County Regulator Affairs
Amendment - 2							
E01: Planning Management	ED	ED+77 days	636	115	$73,140		County Project Manager
E02: FRA Negotiations & Contract Review	ED+77 days	ED+98 days	(52)	115	(5,980)		County Project Manager
E02: FRA Negotiations & Contract Review	ED+77 days	ED+98 days	(80)	94	(7520)		County Regulator Affairs
Additional Project Management			138.5	115	$15,927.50		County Project Manager
					$138,287.50		

*Negotiations support expected to be minimal or not applicable for Fast Track

6. That Schedule C is hereby deleted and is replaced with Schedule C-2, which is attached hereto and incorporated by reference herein.

7. Except as set forth above, there are no other revisions or amendments to the Agreement or to the obligations of the Incumbent or Nextel.

8. In the event of any inconsistencies between the terms and conditions contained in the Agreement and the terms and conditions contained herein, the terms and conditions contained herein shall control.

In WITNESS WHEREOF, the Parties hereto, intending to be legally bound, have duly executed this Amendment as of this _____day of _____2013.

INCUMBENT:	NEXTEL:
Los Angeles County, California	Nextel Operations, Inc.
By: _____	By: _____
Name:	Name: _____
Title:	Title: WILLIAM M JENKINS AUTHORIZED SIGNATORY

APPROVED AS TO FORM:

COUNTY COUNSEL -

By: _____

SCHEDULE C-2

800 MHZ RECONFIGURATION

PLANNING COST ESTIMATE – CERTIFIED REQUEST

Incumbent's Name: Los Angeles, County of, CA

Request for Planning Funding

Pursuant to the Order, Incumbent is required to reconfigure its existing facilities and requests Nextel to fund the following estimated planning costs:

Incumbent Payment Terms: Nextel will pay Incumbent an amount not to exceed the Planning Cost Estimate for Incumbent with respect to each category of work, as set forth below. Nextel will pay Incumbent Eighty Thousand Nine Hundred Seventy-Eight Dollars ($ 80,978) within 15 days (30 days if Incumbent elects to be paid by check rather than electronic funds transfer) after receipt by Nextel of the fully executed Agreement and fully completed Incumbent Information Form (as set forth on Exhibit 1). Nextel will pay any outstanding balance of the Actual Planning Costs due to Incumbent within 30 days after the Planning Funding Reconciliation Date (as "Actual Planning Costs" and "Planning Funding Reconciliation Date" are defined in this Agreement).

Vendor Payment Terms: Nextel will pay each Planning Vendor an amount not to exceed the Planning Cost Estimate for that Planning Vendor with respect to each category of work, as set forth below. Nextel will pay each Planning Vendor within 30 days after receipt by Nextel of (A) an invoice from the Planning Vendor and (B) Incumbent's approval of receipt of goods and services and approval of associated costs included on the Planning Vendor invoice.

Description of Planning Work To Be Performed	**Payee (separately identify Incumbent and each Planning Vendor being paid for work performed)**	**Planning Cost Estimate for Incumbent and each Planning Vendor (Not to exceed listed amount)**
Legal **Amendment – 2:** Additional Legal (See Schedule B for details)	Fletcher, Heald & Hildreth SHULMAN, ROGERS, GANDAL, PORDY & ECKER, P.A.	$33,980.00 $10,875
Frequency Analysis **Amendment – 2:** Reduction (See Schedule B for details)	Los Angeles County Los Angeles County	$23,004.00 ($18,174)
System Inventory	Los Angeles County M/A-COM	$21,091.00 $36,435.00

Amendment – 2: Reduction (See Schedule B for details)	Los Angeles County	($19,711)
Engineering and Implementation Planning **Amendment – 2:** Reduction (See Schedule B for details)	Los Angeles County M/A-COM Los Angeles County	$55,141.00 $161,658.00 ($20,756)
Project Management **Amendment – 2:** Additional (See Schedule B for details)	Los Angeles County M/A-COM Los Angeles County	$62,720.00 $48,379.00 $75,567.50
Other Costs (provide detailed description of nature of cost)		$0.00
Total Estimated Planning Costs		**$470,209.50**

Certification

Pursuant to the Order, Incumbent hereby certifies to the Transition Administrator appointed pursuant to the Order that Incumbent and its Vendors have determined (as listed in Schedule C-2) the minimum funds necessary to support the planning activities in a reasonable, prudent and timely manner, in order to make such rebanded facilities comparable to those presently in use. If applicable, Incumbent further certifies, to the best of Incumbent's knowledge, that any vendor costs listed on Schedule C-2 are comparable to costs that vendor previously charged Incumbent for similar work.

Signature: _____
Print Name: _____
Title: _____
Phone Number: _____
E-mail: _____
Date: _____

COUNTY OF LOS ANGELES

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

RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

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

September xx, 2013

To: Audit Committee

From: Richard Sanchez
Chief Information Officer

REVIEW OF BOARD POLICIES 6.100 - 6.112 - INFORMATION SECURITY

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

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

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

RS:RP:pg

Attachments

c: Chief Executive Officer
Executive Officer, Board of Supervisors

P:\AUDIT COMMITTEE\Review of Policies Memo.docx

DRAFT

ATTACHMENT

INFORMATION TECHNOLOGY SECURITY POLICIES # 6.100 TO 6.112

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

SUMMARY OF REVISIONS	
# 6.105 – Internet Usage	
a)	Reference section revised for currency
b)	Definition Reference section added
c)	First two statements under the Policy section are additions
d)	(NEW) The third statement reflects using Internet for business and non-business purposes
e)	(NEW) The fifth and sixth statements focus on social media and online storage sites
f)	Standardized language for Compliance and Policy Exceptions section
# 6.106 – Physical Security	
a)	Reference section revised for currency
b)	Definition Reference section added
c)	First two statements under the Policy section are additions
d)	Standardized language for Compliance and Policy Exceptions section
# 6.107 – Information Technology Risk Assessment	
a)	Reference section revised for currency, including other related Board Policies
b)	Definition Reference section added
c)	First two statements under the Policy section are additions
d)	Standardized language for Compliance and Policy Exceptions section
# 6.108 – Auditing and Compliance	
a)	Reference section revised for currency, including other related Board Policies
b)	Definition Reference section added
c)	First two statements under the Policy section are additions, and third statement is revised
d)	Standardized language for Compliance and Policy Exceptions section
# 6.109 – Security Incident Reporting	
a)	Reference section revised for currency, including other related Board Policies
b)	Definition Reference section revised
c)	First two statements under the Policy section are additions along with formatting and language revisions
d)	Standardized language for Compliance section
e)	There are no exceptions to this policy
# 6.110 – Protection of Information on Portable Computing Devices	
a)	Reference section revised for currency
b)	Definition Reference section revised
c)	First two statements under the Policy section are additions
d)	(DELETED) Authorization to Place Personal and/or Confidential Information on a Portable Computing Device – this authorization request form was removed from this policy
e)	Numerous policy statements revised due to personal device(s) use
f)	Standardized language for Compliance section
g)	There are no exceptions to this policy
# 6.111 – Information Security Awareness Training	
a)	Reference section revised for currency. including other related Board Policies
b)	Definition Reference section revised
c)	First two statements under the Policy section are additions along with some revisions to the remaining policy statements
d)	Standardized language for Compliance and Policy Exceptions section
# 6.112 – Secure Disposition of Computing Devices	
a)	Reference section revised for currency including other related Board Policies
b)	Definition Reference section added
c)	First two statements under the Policy section are additions
d)	Standardized language for Compliance section
e)	There are no exceptions to this policy

P:\AUDIT COMMITTEE\Board IT Security Policies Summary of Revisions.docx

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

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

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

POLICY

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

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

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

Definitions

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

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

- Portable devices, including, without limitation, personal digital assistants (PDAs), digital cameras, smartphones, cell phones, pagers, and audio/video recorders; and
- Portable storage media, including, without limitation, diskettes, tapes, DVDs, CDs, USB flash drives, memory cards, and external hard disk drives.
  - Multiple user and application computers, including, without limitation, servers;
  - Printing and scanning devices, including, without limitation, printers, copiers, scanners, and fax machines; and
  - Network devices, including, without limitation, firewalls, routers, and switches.

- Telecommunications (e.g., wired and wireless), including, without limitation, voice and data networks, voicemail, voice over Internet Protocol (VoIP), and videoconferencing;
- Software, including, without limitation, application software and operating systems software;
- Information, including, without limitation, the following:
  - Data;
  - Documentation;
  - Electronic mail (e-mail);
  - Personal information; and
  - Confidential information.
- Services, including, without limitation, hosted services and County Internet services; and
- Systems, which are an integration and/or interrelation of various components of County IT resources to provide a business solution (e.g., eCAPS).

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

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

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

As used in this Policy, the term "County IT security incident" includes any actual or suspected adverse event (e.g., virus/worm attack, loss or disclosure of personal information and/or confidential information, disruption of data or system integrity, and disruption or denial of availability) relating to any County IT security.

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

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

General

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

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

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

RESPONSIBILITIES

~~Departments, Commissions, Board and Offices~~

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

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

County Departments

The head of each County department is responsible for ensuring County IT security, including, without limitation, within the County department. Management of each

County department is responsible for organizational adherence to Countywide County IT resources policies, standards, and procedures and Countywide County IT security policies, standards, and procedures, as well as any additional policies, standards, and procedures established by the County department. They shall ensure that all County IT users are made aware of those policies, standards, and procedures and that compliance is mandatory.

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

Chief Information Office (CIO)

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

Chief Information Security Officer (CISO)

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

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

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

County Department IT Management/Departmental Chief Information Officer

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

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

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

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

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

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

Departmental Information Security Officer (DISO)

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

- Manage security of ~~information technology assets~~ County IT resources within the County department;
- Assist in the development of ~~departmental information technology~~ County department IT security policy~~ies;~~
- Regularly represent the County department at the ~~Information Security Steering Committee~~ (ISSC~~)~~ meetings;
- ~~Coordinate~~ Lead the Departmental Computer Emergency Response Team (DCERT); and
- Report County IT security incidents to the CISO, as required by County IT security policies, standards, and procedures.

~~Employees and Other Authorized Users~~ County Users

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

Information Security Steering Committee ~~(ISSC)~~

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

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

- Assisting the CISO in developing, reviewing, and recommending ~~information~~ Countywide County IT security policies;
- Identifying and recommending industry best practices for ~~information~~ Countywide County IT security;
- Developing, reviewing, ~~and~~ recommending, and approving Countywide County IT security standards, procedures and guidelines;
- Coordinating ~~inter-departmental~~ communication and collaboration among County departments on Countywide and County department IT security issues; and
- Coordinating Countywide 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 IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

Requests for exceptions to this Board of Supervisors (Board) Policy ~~must~~ shall be reviewed by the CISO and the CIO, and shall require approv~~ed~~al by the Board ~~of Supervisors~~. County departments requesting exceptions ~~should~~ shall provide such

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004 **Sunset Date: July 13, 2008**

Reissue Date: **Sunset Review Date:**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

County Policy of Equity

~~Acceptable Use Agreement (Attached)~~

POLICY

General

This policy is applicable to all County IT users.

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

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

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

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

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

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

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

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

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

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

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

~~user's duty to use the County's resources responsibly, professionally, ethically, and lawfully.~~

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

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

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

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

~~Definitions~~

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

- ~~Computers and any electronic device which stores and/or processes County data (for example: desktops, laptops, midrange, mainframes, PDAs, County wired or wireless networks, digital cameras, copiers, IP phones, faxes, pagers, related peripherals, etc.)~~

- ~~Storage media (diskettes, tapes, CDs, zip disk, DVD, etc.) on or off County premises.~~

- ~~Network connections (wired and wireless) and infrastructure, including jacks, wiring, switches, patch panels, hubs, routers, etc.~~

- ~~Data contained in County systems (databases, emails, documents repositories, web pages, etc.)~~

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

Access Control

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

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

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

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

Authentication

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

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

County ~~information technology resource~~ IT users shall not allow others to access a system while it is logged on under their user sessions. The only exceptions allowed are when the software cannot be configured to enforce a login, 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 ~~information technology resource~~ users shall be responsible for the integrity of the authentication mechanism granted to them. For example, County IT users shall not share their computer identification codes ~~passwords, electronic cards, biometric logons, secure ID cards~~ and~~/or~~ other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, SecurID cards/tokens, biometric logons, and smartcards). ~~with others.~~

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

~~Data~~Information Integrity

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

Accessing County IT ~~Technology~~ Resources Remotely

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

Privacy

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

Confidentiality

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

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

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

~~(See Acceptable Use Agreement)~~

RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:

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

ANNUAL

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

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

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

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

1. Computer crimes: I am aware of California Penal Code Section 502(c) -Comprehensive Computer Data Access and Fraud Act (set forth, in part, below ~~attached~~). I shall ~~will~~ immediately report ~~any suspected computer misuse or crimes~~ to my management any suspected misuse or crimes relating to County IT resources or otherwise.

2. County IT security incident reporting: I shall notify the County Department's Help Desk and/or Departmental Information Security Officer (DISO) as soon as a County IT security incident is suspected.

3. Security access controls: I shall ~~will~~ not subvert or bypass any security measure or system which has been implemented to control or restrict access to County IT resources and any related restricted work areas and facilities. ~~computers, networks, systems or data.~~ I shall ~~will~~ not share

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

4. Passwords: I shall not keep or maintain any unsecured record of my password(s) to access County IT resources, whether on paper, in an electronic file, or otherwise. I shall comply with all County and County department policies relating to passwords. I shall immediately report to my management any compromise or suspected compromise of my password(s) and have the password(s) changed immediately.

5. Approved business purposes: I shall ~~will~~ use the County~~'s Information Technology (~~IT resources ~~) assets including computers, networks, systems and data~~ for County management approved business purposes only. I understand that my use of County IT resources is subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time. I understand that if my actions result in access to County IT resources from any of my personally owned computing devices (e.g., laptop, home desktop computer, personal digital assistant (PDA), smartphone, cell phone, and USB flash drives), such devices are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time.

6. Approved devices: I shall obtain written departmental management approval that includes, minimally, the Departmental Information Security Officer (DISO), for any computing device not owned or provided by the County prior to accessing and/or storing County IT resources.

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

8. Confidentiality: I shall ~~will~~ not access, store, or disclose to any person ~~County program code, data, information or documentation to any individual~~ or organization any County IT resources (e.g., software code; business data, documentation, and other information; personal data, documentation, and other information; and confidential data, documentation, and other information), unless specifically authorized to do so by County management. ~~the recognized information owner.~~

9. Computer virus and other malicious devices ~~code:~~ I shall ~~will~~ not intentionally introduce any malicious device (e.g., computer virus, spyware, and ~~worms or~~ malicious code), into any County IT resources. ~~computer, network, system or data.~~ I shall not use County IT resources to intentionally introduce any malicious device into any County IT resources or any non-County IT systems or networks. I shall ~~will~~ not disable, modify, or delete computer security software (e.g., antivirus software, 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. ~~virus detection and eradication software on County computers, servers and other computing devices I am responsible for.~~

10. Offensive materials: I shall ~~will~~ not access, create, or distribute ~~send any offensive materials,~~ (e.g., via e-mail) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County IT resources (e.g., over County-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless it is in the performance of my assigned job duties (e.g., law enforcement). I shall report to my management any offensive materials observed or received by me on County IT resources. ~~sexually explicit, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.~~

11. Internet: I understand that the Internet is public and uncensored and contains many sites that may be considered offensive in both text and images. I shall use County Internet services for County management approved business purposes only (e.g., as a research tool or for e-mail communication). I understand that County Internet services may be filtered, but in my use of them, I may be exposed to offensive materials. I agree to hold County harmless from and against any and all liability and expense should I be inadvertently exposed to such offensive materials.

12. E-mail and other information: I understand that County e-mail and other information, in either electronic or other forms, may be logged/stored, are a public record, and are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time. I shall comply with all County e-mail use policies, standards, and procedures and use proper business etiquette when communicating over e-mail systems.

13. Activities related to County IT resources: I understand that my activities related to County IT resources (e.g., use of e-mail, instant messaging, blogs, electronic files, County Internet services, and County systems) may be logged/stored, are a public record, and are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time. I do not expect any right to privacy concerning my activities related to County IT resources, including, without limitation, in anything I create, store, send, or receive using County IT resources. I shall not intentionally, or through negligence, damage, interfere with the operation of, or prevent authorized access to, County IT resources and shall use County IT resources responsibly, professionally, ethically, and lawfully.

14. Public forums ~~Internet~~: I shall not use County IT resources to create, exchange, publish, distribute, or disclose in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions). ~~I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services may be filtered but in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be inadvertently exposed to~~

~~such offensive materials. I understand that my Internet activities may be logged, are a public record, and are subject to audit and review by authorized individuals.~~

15. Internet storage sites: I shall not store County information on any Internet storage site without understanding the potential risk. ~~Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will comply with County e-mail use policy and use proper business etiquette when communicating over e-mail systems.~~

16. Copyrighted and other proprietary materials: I shall ~~will~~ not copy or otherwise use any copyrighted or other proprietary materials (e.g., licensed software and documentation), except as permitted by the applicable license agreement and approved by County management. ~~any licensed software or documentation except as permitted by the license agreement.~~

17. Compliance with County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements: I shall comply with all applicable County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements relating to County IT resources. These include, without limitation, Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy, Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, and Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

18. Disciplinary action and other actions and penalties for non-compliance: I understand that my non-compliance with any provision ~~portion~~ of this Agreement may result in disciplinary action and other actions (e.g., ~~including my~~ suspension, discharge, denial of access, and termination of contracts), as well as both civil and criminal penalties and that County may seek all possible legal redress. ~~service, cancellation of contracts or both civil and criminal penalties~~

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

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

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

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongly control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or

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

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

_____	_____
County IT User's Name	County IT User's Signature
_____	_____
County IT User's Employee/ID Number	Date
_____	_____
Manager's Name	Manager's Signature
_____	_____
Manager's Title	Date

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

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

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 ~~Policy~~ – ~~Information Technology~~ IT and Security Policies

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

POLICY

This policy is applicable to all County IT users.

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

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

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

computing device.

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

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

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

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

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

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

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

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

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

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

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

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

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

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004 **Sunset Date: July 13, 2008**

Reissue Date: **Sunset Review Date:**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

POLICY

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

The County shall establish a Countywide Computer Emergency Response Team (CCERT). The CCERT will be led by the Chief Information Security Officer (CISO) and ~~will~~ shall consist of representatives from all County departments. CCERT ~~will~~ shall

communicate security information, guidelines for notification processes, identify potential security risks, and coordinate responses to thwart, mitigate, or eliminate ~~a countywide computer~~ security threats to County IT resources.

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

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

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

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

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

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

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

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

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

Definition Reference

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

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

POLICY

This policy is applicable to all County IT users.

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

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

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

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

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

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

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

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

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

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

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

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

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

Definition Reference

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

County Policy of Equity

POLICY

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

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

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

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

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

No County IT user shall use County IT resources to create, exchange, publish, or distribute in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal and confidential information, political lobbying, religious promotion, and opinions).

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

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

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

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

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

Monitoring and/or investigating the access to, and use of, County IT resources by County IT users shall require approval by County management. If evidence of abuse is identified, County department management shall immediately report the incident to the Auditor-Controller, Office of County Investigations.

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

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

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

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

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

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

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

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

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

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

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

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

- ~~Using the County's Internet services for the unauthorized downloading of software or file sharing software that is not specifically used for conducting County business.~~

- ~~Using the County's Internet services for downloading or distributing material in violation of copyright laws (i.e., movies, music, software, books, etc.).~~

- ~~Using the County's Internet services for downloading or distributing pornography or other sexually explicit materials.~~

- ~~Using the County's Internet services for any activities that could be construed as a violation of National/Homeland Security laws.~~

- ~~Using the County's Internet services to post scams such as pyramid schemes or "make-money-fast" schemes to others via the Internet.~~

- ~~Using the County's Internet services to post or transmit any message or material which is libelous, defamatory, or which discloses private or personal matters concerning any person or group.~~

- ~~Using County Internet services for running a private business or web site.~~

- ~~Using the County's Internet services to post or transmit to unauthorized individuals any material deemed to be private, proprietary, or confidential information.~~

- ~~Attempting an unauthorized access to the account of another individual or group on the Internet, or attempting to penetrate beyond County security measures or security measures taken by others connected to the Internet, regardless of whether or not such intrusion results in corruption or loss of data.~~

- ~~Knowingly or carelessly distributing malicious code to or from County information technology resources.~~

- ~~Using the County's Internet services to participate in partisan political activities.~~

Definition Reference

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

POLICY

This Policy is applicable to all County IT users.

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

Facility Security Plan

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

Proper Identification

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

Access to Restricted IT Areas

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

Physical Security Controls

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

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

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

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

~~Equipment Control~~

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

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

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

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

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004 **Sunset Date: July 13, 2008**

Reissue Date: **Sunset Review Date:**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

POLICY

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

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

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

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

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

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

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

Definition Reference

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

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

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

Compliance

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

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004 **Sunset Date: July 13, 2008**

Reissue Date: **Sunset Review Date:**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

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

REFERENCE

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

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

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

POLICY

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

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

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

This Policy is applicable to all County IT users.

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

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

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

Definition Reference

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

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

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

Compliance

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

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

other actions, as well as both civil and criminal penalties.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004 **Sunset Date: July 13, 2008**

Reissue Date: **Sunset Review Date:**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

May 8, 2007, Board Order No. 26 – Board of Supervisors – Information Security Policies

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

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

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

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

POLICY

This Policy is applicable to all County IT users.

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

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

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

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

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

responsibilities for the Auditor-Controller.

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

Chief Information Security Officer (CISO)

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

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

Chief HIPAA Privacy Officer (CHPO)

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

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

Office of County Investigations (OCI)

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

- System breaches from internal or external sources;
- Lost or stolen computing devices containing personal information and/or confidential information; ~~and data~~
- Inappropriate non-work related ~~data~~ information, which may include, without limitation, pornography, music, and videos; and
- Actual or suspected loss or disclosure of personal information and/or confidential information.

Chief Information Office (CIO)

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

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

Definition Reference

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

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

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

Security Policy.

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

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

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

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

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

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

Compliance

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

Policy Exceptions

There are no exceptions to this Policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007
Reissue Date:

Sunset Review Date: May 8, 2011
Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

May 8, 2007, Board Order No. 26 – Board of Supervisors – Information Security Polices

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

County Policy of Equity

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

POLICY

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

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

~~Definition Reference~~

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

-

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

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

-

~~Full Encryption of All Information on all Portable Computing Devices~~

~~Security measures must be employed by all County departments to safeguard all Personal and/or Confidential information on all portable computing devices. All County-~~

~~owned or provided portable computers (e.g., laptops and tablet computers) must at all times have automatic full disk encryption that does not require user intervention nor allow user choice to implement. If Personal and/or Confidential information is placed on any portable computing devices, all such information must be encrypted while on those portable computing devices.~~

-

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

~~• Portable computers, such as laptops and tablet computers~~

~~• Portable devices, such as Personal digital assistants (PDA), digital cameras, portable phones, and pagers~~

~~• Portable storage media, such as diskettes, tapes, CDs, zip disks, DVDs, flash memory/drives, and USB drives~~

-

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

~~Personal and/or Confidential Information~~

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

-

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

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

A) Portable Computing Devices and Information

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

The County prohibits the unnecessary placement (download or input) of Personal information and/or Confidential information on portable computing devices. However, County IT users, who in the course of County business, must place Personal information and/or Confidential information on portable computing devices, shall be

made aware of the risks involved and impact to the affected person/entities in the event of actual or suspected loss or disclosure of Personal information and/or Confidential information.

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

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

B) Protection Requirements for Stored Information

County Departments must safeguard all Personal information and/or Confidential information on all portable computing devices.

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

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

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

C) Limit Exposure of Stored Information

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

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

Any actual or suspected loss or disclosure of Personal information and/or Confidential

information shall be reported under Board of Supervisors Policy No. 6.109 – Security Incident Reporting. In all cases, every attempt shall be made to assess the impact of storing, and to mitigate the risk to, Personal information and/or Confidential information on all portable computing devices.

Definition Reference

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

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

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

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

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

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

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

Compliance

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

Policy Exceptions

There are no exceptions to this Policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007

Sunset Review Date: May 8, 2011

Reissue Date:

Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

May 8, 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

POLICY

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

~~employment with the County.~~

This Policy is applicable to all County IT users.

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

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

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

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

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

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

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

Information security awareness training shall be provided to County IT users

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

Definition Reference

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

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

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

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

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

Compliance

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

Policy Exceptions

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

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007
Reissue Date:

Sunset Review Date: May 8, 2011
Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

October 23, 2007, Board Order No. 22 – Board of Supervisors – Information Technology and Security Policy

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

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

~~Chief Information Officer's Memo "Countywide Information Technology and Security Policy"~~

Board of Supervisors Policy 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information

POLICY

This policy is applicable to all County IT users.

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

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

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

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

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

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

~~• Personal computers, such as desktops, laptops, and personal digital assistants (PDA)~~

~~• Multiple user and application computers, such as servers~~

~~• Portable storage media, such as diskettes, tapes, CDs, zip disks, DVDs, flash memory/drives, and USB drives~~

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

• Computing device sent to salvage;
• Computing device destroyed; and
• Computing device donated to a non-County organization.

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

There are no exemptions to this Policy.

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: October 23, 2007
Reissue Date:

Sunset Review Date: October 23, 2011
Sunset Review Date: