



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

WILLIAM T FUJIOKA
Chief Executive Officer

REVISED

DATE: September 19, 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 – APPROVAL OF A SOLE SOURCE AGREEMENT WITH NETSCOUT SYSTEMS, INC.**
DHS/CIO – Mitchell H. Katz and Richard Sanchez or designee(s)
 - B) **Board Letter – JOB ORDER CONTRACTS FOR MAINTENANCE, REPAIR, AND REFURBISHMENT OF COUNTY INFRASTRUCTURE AND FACILITIES ADOPT AND ADVERTISE VARIOUS SPECIFICATIONS, AWARD CONTRACTS**
ISD – Jim Jones or designee
 - C) **Board Letter – ORDINANCE ESTABLISHING A DISABLED VETERAN BUSINESS ENTERPRISE PREFERENCE PROGRAM**
ISD – Jim Jones or designee
 - D) **Board Letter – APPROVAL FOR INTERIM ORDINANCE AUTHORITY AND APPROPRIATION ADJUSTMENT FOR ADMINISTRATIVE SUPPORT OF THE L.A. MEMORIAL COLISEUM COMMISSION**
Executive Office, BOS – Sachi A. Hamai or designee
 - E) **Review of IT Board Policies No. 6.100 through 6.112**
(DISCUSSION CONTINUED FROM 9/12/13 OPS MEETING)
CIO – Richard Sanchez or designee
2. Public Comment
3. Adjournment

Date: October 15, 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:

**APPROVAL OF A SOLE SOURCE AGREEMENT WITH
NETSCOUT SYSTEMS, INC
(ALL SUPERVISORIAL DISTRICTS)
(3 VOTES)**

CIO RECOMMENDATION: APPROVE []

SUBJECT

Approval of a new Sole Source Agreement with NetScout Systems, Inc for the provision of Maintenance and Support services for existing NetScout hardware and software installed to monitor enterprise network telecommunications and applications in the Department of Health Services.

IT IS RECOMMENDED THAT THE BOARD:

1. Authorize the Director of Health Services (Director), or his designee, to execute a sole source Agreement with NetScout Systems, Inc ("NetScout") to provide maintenance and support services for existing NetScout hardware and software effective upon execution by the parties for the period of November 13, 2013 through November 12, 2014 with a maximum obligation of \$160,894.
2. Delegate authority to the Director, or his designee, to execute amendments as needed in order to add any relevant new or updated County contract terms; to delete equipment and to increase the maximum obligation for hardware and software maintenance and support by no more than 10% of the maximum obligation during the period.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTIONS

The Department of Health Services (DHS) currently obtains maintenance and support services from NetScout under a Purchase Order (PO) issued by the Internal Services Department (ISD). ISD has advised DHS to seek Board approval for an Agreement for maintenance and support services for NetScout hardware and software products purchased under a PO because the cost of services sought by DHS exceeds ISD's PO authority.

Approval of the first recommendation will allow the Director or his designee, to execute an Agreement substantially similar to Exhibit I, with NetScout to ensure continuation of the maintenance and support service.

Approval of the second recommendation will enable the Director to amend the Agreement to: (1) add, delete and/or change non-substantive terms and conditions in the Agreement; (2) to add/delete equipment for hardware and software maintenance; and (3) will allow the Director to Increase the total maximum obligation by no more than 10 percent, a Maximum Obligation of \$176,973.

Implementation of Strategic Plan Goals

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

FISCAL IMPACT/FINANCING

The total maximum obligation is \$160,894. The total potential increase under the 10 percent delegated authority is \$16,089 and would be funded using existing resources.

Funding is included in DHS' Fiscal Year 2013-14 Final Budget and will be requested in future fiscal years.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

NetScout monitors performance of: servers, routers, switches, storage area networks (SANs), plus various enterprise devices and applications. A unique functionality of NetScout is the predicative alarming of devices monitored to avoid disruptions. Employing NetScout equipment and maintenance services has enabled DHS to provide uninterrupted patient-care data and network applications to support patient care. Additionally, NetScout supports continuous video conferencing and voice-over-internet-protocol (VOIP) services for the enterprise. This functionality is essential for DHS operations and enterprise telecommunications.

Use of NetScout monitoring equipment began seven (7) years ago at USC Medical Center to support computer networks and applications. In November 2009, DHS deployed NetScout to monitor performance of network architectures and enterprise applications at Health Services Administration (HSA), and all DHS Medical Center facilities.

The recommended Agreement includes all of the Board of Supervisors' required provisions as well as County standard IT provisions applicable to Maintenance and Support service. County Counsel has approved Exhibit I as to form.

The NetScout Agreement is not a Proposition A service agreement. It is the acquisition of infrastructure maintenance and support authorized by Government Code section 31000.

CONTRACTING PROCESS

NetScout offered a superior product. One NetScout product could do the job of two (2) similar vendor products. Also, NetScout offered the unique service of performing predicative monitoring of network attached devices and applications for possible disruptions. With predicative monitoring, DHS staff has been able to maintain network and application availability without disruptions or delay of critical patient data services. NetScout's position as the Original Equipment Manufacture (OEM) of the hardware and software products make it uniquely qualified to maintain and support its proprietary products. NetScout is the only company that can warranty the work of NetScout staff and technicians for the repair and maintenance of existing NetScout proprietary products already implemented at DHS facilities.

Attachment A is the sole source checklist in compliance with Board Policy 5.100.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of the recommendations will ensure that DHS can provide uninterrupted: critical patient-care data, patient application services, medical recordkeeping, and DHS enterprise communication.

Respectfully submitted,

Reviewed by:

Mitchell H. Katz, M.D.
Director

Richard Sanchez
Chief Information Officer

MHK: rt

Enclosures ()

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



JIM JONES
Acting Director

County of Los Angeles
INTERNAL SERVICES DEPARTMENT

1100 North Eastern Avenue
Los Angeles, California 90063

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:

**JOB ORDER CONTRACTS
FOR MAINTENANCE, REPAIR, AND REFURBISHMENT
OF COUNTY INFRASTRUCTURE AND FACILITIES
ADOPT AND ADVERTISE VARIOUS SPECIFICATIONS, AWARD CONTRACTS
(ALL DISTRICTS) (3 VOTES)**

SUBJECT

This action is to adopt the Job Order Contract (JOC) Unit Price Book and Specifications; approve for advertisement bids to be received; award agreements to the Lowest Responsive and Responsible Bidders for 10 separate JOC agreements.

IT IS RECOMMENDED THAT YOUR BOARD:

1. Find that the adoption of the JOC Unit Price Book and Specifications, advertisement for bids and award of JOCs are exempt from the California Environmental Quality Act, for the reasons stated in this letter and in the record of the action.
2. Adopt the October 2013 JOC Unit Price Book and Specifications.
3. Instruct the Executive Officer of the Board to advertise for bids to be received for ten separate JOCs in accordance with the Instruction Sheet for Publishing Legal Advertisements (Attachment I).

4. Authorize the Acting Director of Internal Services Department (ISD) or his designee to prepare, award and execute six general, four specialty (two electrical, and two mechanical) JOC agreements to provide services to County facilities such as as-needed repair, deferred maintenance, and refurbishments. The agreements are for a one-year term effective on contract execution. JOC111, JOC112, JOC113, JOC114, JOC115, JOC116, EJOC33, EJOC34, MJOC30, and MJOC31 are not-to-exceed \$4.4 million each. The aggregate not-to-exceed amount for the ten agreements is \$44 million.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

Approval of the recommended action will find that adoption of the JOC Unit Price Book and Specifications, advertisement for bids and award of JOCs are exempt from the California Environmental Quality Act (CEQA) and will augment ISD's ability to effectively and efficiently maintain and repair (including emergency repairs) County infrastructure and facilities.

JOCs are flexible, cost-effective unit price contracting method to accomplish maintenance, repair, and refurbishment of County infrastructure and facilities without extensive plans and specifications. JOCs are annual contracts that may be awarded for repair, remodeling, refurbishment, or other repetitive work, but not for new construction. This process reduces administrative requirements and lowers direct construction costs while meeting all federal, State, and County procurement requirements.

Implementation of Strategic Plan Goals

This action meets the County's Strategic Plan Goal No. 1 for Operational Effectiveness by providing timely facilities services, effectively managing County resources and investing in public infrastructure.

FISCAL IMPACT/FINANCING

Maintenance, repair, and refurbishment work will be funded through the appropriate maintenance, capital, refurbishment, or infrastructure project budgets. ISD's Fiscal Year 2013-14 Adopted Budget includes \$44 million for these JOC agreement expenditures. ISD will only incur JOC expenditures to the extent that they are offset through County department and Contract Cities billings and within available appropriation. For capital projects, no work will be assigned to these JOCs without authorization from the Chief Executive Office. There are no minimum obligations on these contracts.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

Board approval of the recommended actions is required by Public Contract Code Sections 20124 and 20125.

Public Contract Code Section 20128.5 allows individual JOCs to have a one-year term and a maximum value of \$4.4 million. A 1997 amendment to the Public Contract Code allows annualized increases in the maximum contract value, based on the California Consumer Price Index.

The terms and conditions of the recommended contracts will be approved as to form by County Counsel prior to execution and will contain the Board's required contract provisions including those pertaining to consideration of qualified County employees targeted for layoffs as well as qualified GAIN/GROW participants for employment openings, compliance with the Jury Service Ordinance, Safely Surrendered Baby Law, the Child Support program, Defaulted Tax Program Ordinance, and the Local Worker Program. The JOC Agreements are not Proposition "A" contracts and therefore are not subject to the County's Living Wage Program.

Data regarding the proposers' minority participation will be on file with ISD. The contractors will be selected upon final analysis and consideration without regard to race, creed, gender, or color.

The General Conditions and October 2013 Unit Price Book and Specifications include the contractual provisions, methods, and material requirements necessary for this project and are on file with ISD.

ENVIRONMENTAL DOCUMENTATION

The recommended action, to adopt the Job Order Contract Unit Price Book and Specifications, advertise for bids and award of JOCs are categorically exempt from CEQA. JOC projects include repair, maintenance and refurbishment of existing structures and facilities as requested by County departments, which are generally categorically exempt under Section 15301, Class 1, of the State CEQA Guidelines. The proposed work involves either negligible or no expansion of existing use, and any replacement structures will have substantially the same purpose and capacity as structures replaced. ISD will file all required Notices of Exemption for each categorically exempt project as required by CEQA. For any work that is not determined to be exempt from CEQA following further assessment, the Department will return to the Board to recommend approval of the appropriate environmental documentation pursuant to CEQA prior to implementation of applicable work orders under the JOCs.

CONTRACTING PROCESS

The Executive Officer of the Board will advertise the JOC invitation for bids in various publications throughout the County of Los Angeles. Additionally, ISD will advertise the invitation for bids on the Green Sheet publication and post the bids on the County's "Doing Business with Us" web site.

The recommended JOCs will be solicited on an open-competitive basis and in accordance with applicable federal, State, and County requirements. The County will award contracts to the lowest responsive and responsible bidder pursuant to the State Public Contract Code.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

The use of these contracts will expedite the completion of maintenance, repair, and refurbishment of County infrastructure and facilities work managed by ISD. Minor impacts to tenant departments may occur while maintenance, repair, and refurbishment of County infrastructure and facilities work is underway.

There is no employee impact. JOCs are intended to augment, but not replace the County workforce, and to ensure our ability to respond to emergent requirements.

CONCLUSION

Upon Board approval, please return one adopted stamped copy of this letter to ISD.

Respectfully submitted,

Jim Jones
Acting Director

Attachments

c: Chief Executive Officer
County Counsel

ATTACHMENT I

**INTERNAL SERVICES DEPARTMENT: JOB ORDER CONTRACTS
FOR MAINTENANCE, REPAIR, AND REFURBISHMENT
OF COUNTY INFRASTRUCTURE AND FACILITIES
ADOPT AND ADVERTISE VARIOUS SPECIFICATIONS, AWARD CONTRACTS
(ALL DISTRICTS) (3 VOTES)**

PUBLISHING LEGAL ADVERTISEMENTS: In accordance with the State of California Public Contract Code Section 20125, you may publish once a week for two weeks in a weekly newspaper, or ten times in a daily newspaper. However, the first publication must appear at least 10 days prior to the bid opening date. Forward three reprints of this advertisement to Alterations & Improvements Division, Internal Services Department, 1100 Eastern Avenue, Los Angeles, California 90063.

**OFFICIAL NOTICE
INVITING BIDS**

Notice is hereby given that Internal Services Department (ISD) will receive sealed bids for furnishings, materials, labor, and equipment required to complete construction for the following work:

<u>SPECS.</u>	<u>PROJECT</u>	<u>BID DOC. FEE</u>	<u>BID DEADLINES</u>	
			<u>DATE</u>	<u>TIME</u>
JOC Specs.	JOC 111	\$50.00 each	11/12/2013	10:00 a.m.
JOC Specs.	JOC 112	\$50.00 each	11/12/2013	10:00 a.m.
JOC Specs.	JOC 113	\$50.00 each	11/12/2013	10:00 a.m.
JOC Specs.	JOC 114	\$50.00 each	11/12/2013	10:00 a.m.
JOC Specs.	JOC 115	\$50.00 each	11/12/2013	10:00 a.m.
JOC Specs.	JOC 116	\$50.00 each	11/12/2013	10:00 a.m.
JOC Specs.	EJOC 33	\$50.00 each	11/12/2013	10:00 a.m.
JOC Specs.	EJOC 34	\$50.00 each	11/12/2013	10:00 a.m.
JOC Specs.	MJOC 30	\$50.00 each	11/12/2013	10:00 a.m.
JOC Specs.	MJOC 31	\$50.00 each	11/12/2013	10:00 a.m.

Copies of the project manual and technical specifications may be obtained at the **mandatory** Pre-bid Conference or Internal Services Department Bid Office located at 1100 N. Eastern Avenue, Los Angeles, California, 90063 for the fee stated above. For bid information, please call (323) 267-3129 or (323) 267-2243. Each bid shall be submitted on the required form sealed and filed at the Bid Office located at the first floor of 1100 N. Eastern Avenue, Los Angeles, CA 90063 no later than 10:00 a.m. on the date indicated above. Bids will be publicly opened, examined, and declared by ISD JOC Contract Administration approximately 30 minutes following the deadlines for

Attachment I
October 8, 2013
Page 2

submission of bids stated above in Conference Room G101, 1100 N. Eastern Avenue, Los Angeles, CA 90063.

Bidders must comply with the provisions of the Bidding Requirements and General Conditions concerning bid guarantee, contract bonds, and insurance requirements. These projects require the prime contractor to possess a "B" license at time of bid for General Contract JOCs (JOC111, JOC112, JOC113, JOC114, JOC115, JOC116). Contractors bidding Electrical JOCs (EJOC33, EJOC34) are required to possess a "C-10" license at time of bid. Contractors bidding the Mechanical JOCs (MJOC30, MJOC31) are required to possess a "C-20" and "C-36" license at time of bid. Contractor should verify to his/her satisfaction that he/she holds the correct license for this type of project.

PREBID CONFERENCE

ISD will hold a single **mandatory** pre-bid conference for all of the listed Job Order Contract (JOC) contracts/projects at 10:00 a.m. on October 28, 2013, Conference Room G101 at 1100 N. Eastern Avenue, Los Angeles, CA 90063 to provide information on the JOC, bidding process, and answer any questions that potential bidders may have. A bid submitted by a company that did not have a representative of the company sign in as being present at the mandatory pre-bid conference will be rejected as non-responsive, and it is strongly recommended that the representative who attends the mandatory pre-bid conference for the company be a principal of the company or a person authorized to make decisions for the company. For further directions, please contact Ms. Sue Chang at (323) 267-3129 or Ms. Jane Lee at (323) 267-2243.

OTHER INSTRUCTIONS

The County supports and encourages equal opportunity contracting. The contractor shall make good faith efforts, as defined in Section 2000 of the Public Contract Code, relating to contracting with Community Business Enterprises.

The Board of Supervisors reserves the right to reject any or all bids or to waive technical errors and discrepancies in bids submitted in the public's interest.

Si necesita información en español, por favor llame al telefono (323) 267-2864.



Upon 72 hours notice, ISD can provide program information and publication in alternate formats or make other accommodations for people with disabilities. In addition, program documents are available at our office in Los Angeles (1100 N. Eastern Avenue, Los Angeles), which is accessible to individuals with disabilities. To request accommodations ONLY, or for more ADA information, please contact our departmental ADA Coordinator at (323) 267-2432, Monday through Thursday, from 7:00 a.m. to 5:30 p.m.



Con 72 horas de notificación, ISD puede proporcionar información y publicaciones sobre el programa y formas alternas o hacer otras comodidades para gente incapacitada. Además, documentación sobre el programa está disponible en nuestra oficina principal en Los Angeles (1100 N. Eastern Avenue, Los Angeles) lo cual es accesible para individuos con incapacidades. Para solicitar comodidades SOLAMENTE, o para mas información del ADA, pongase en contacto con nuestro Coordinador del ADA del departamento al (323) 267-2432, de Lunes a Jueves de 7:00 a.m. a 5:30 p.m.

By order of the Board of Supervisors of the County of Los Angeles, State of California, dated October 8, 2013.

SACHI A. HAMAI, EXECUTIVE OFFICES
OF THE BOARD OF SUPERVISORS
OF THE COUNTY OF LOS ANGELES



JIM JONES
Acting Director

County of Los Angeles
INTERNAL SERVICES DEPARTMENT

1100 North Eastern Avenue
Los Angeles, California 90063

Telephone: (323) 267-2103
FAX: (323) 264-7135

"To enrich lives through effective and caring service"

October 15, 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:

**ORDINANCE ESTABLISHING A DISABLED VETERAN BUSINESS ENTERPRISE
PREFERENCE PROGRAM
(ALL SUPERVISORIAL DISTRICTS)
(3 VOTES)**

SUBJECT

Approval of an ordinance establishing Chapter 2.211 to Title 2 – Administration of the County Code, Disabled Veteran Business Enterprise Preference Program.

IT IS RECOMMENDED THAT YOUR BOARD:

Approve an ordinance establishing Chapter 2.211 to Title 2 – Administration of the County Code, Disabled Veteran Business Enterprise Preference Program.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

On August 20, 2013, your Board directed the Internal Services Department (ISD) to work with County Counsel to prepare an ordinance ("Ordinance") amending the County Code, Title 2 – Administration, to establish a Disabled Veteran Business Enterprise (DVBE) Preference Program that provides for a purchasing and contracting bid preference to veterans with service-connected disabilities.

The proposed Ordinance (attached) establishes a DVBE Preference Program ("DVBE Program") that is consistent with other preference programs established by the Board, including the Local Small Business Enterprise (LSBE), and Transitional Job Opportunities Preference (TJOP) programs.

These programs are designed to promote inclusiveness and economic development to ensure that all businesses are provided equal opportunities in the County's purchasing and contracting activities.

Consistent with the other County preference programs, the proposed DVBE Program provides for an eight percent (8%) price or scoring preference to bids and proposals from qualified DVBEs. A qualified business is one that has been certified as a DVBE by the State of California or the Veteran's Administration at the time of bid or proposal submittal.

The DVBE Program exclusions are also consistent with the other County preference programs. The DVBE Program excludes any contract or purchase for which a federal, State or local law prohibits or limits a DVBE preference. Furthermore, as a DVBE may also be certified LSBE or TJOP, the Ordinance restricts any preference amount to a maximum of eight percent (8%).

If approved by your Board, the proposed Ordinance will be implemented in countywide solicitations released on or after December 1, 2013. This will provide ISD sufficient time to update the website and provide implementation instructions to County departments, and communicate the DVBE Program to the business community, including potential DVBE vendors.

Implementation of Strategic Plan Goals

Approval of the proposed addition to the County Code will further the County's Strategic Plan Goal of Organizational Effectiveness by ensuring that service delivery systems are efficient, effective and goal-oriented.

FISCAL IMPACT/FINANCING

There is no historical or financial information available for DVBEs that are currently doing business with the County. However, State records indicate that there are 125 such businesses that are located in Los Angeles County.

ISD believes that establishing a preference would generate DVBE participation, and the preference amount would result in awards to DVBEs. However, given the limited number of DVBEs identified in the region, ISD estimates that the overall increase in countywide costs would be marginal. No cost is incurred when a DVBE is the low bidder.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The proposed Ordinance has been approved as to form by County Counsel.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

The proposed Ordinance will enhance existing contracting and purchasing policies and procedures while providing the appropriate guidance and direction necessary to reach decisions that are consistent with your Board's direction.

Respectfully submitted,

Jim Jones
Acting Director

TT:JS:j

Attachment

c: Chief Executive Officer
County Counsel
Executive Officer, Board of Supervisors
Small Business Commission



SACHI A. HAMAI
EXECUTIVE OFFICER

COUNTY OF LOS ANGELES BOARD OF SUPERVISORS

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

MEMBERS OF THE BOARD

GLORIA MOLINA

MARK RIDLEY-THOMAS

ZEV YAROSLAVSKY

DON KNABE

MICHAEL D. ANTONOVICH

September 24, 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:

APPROVAL FOR INTERIM ORDINANCE AUTHORITY AND APPROPRIATION ADJUSTMENT FOR ADMINISTRATIVE SUPPORT OF THE LOS ANGELES MEMORIAL COLISEUM COMMISSION (ALL DISTRICTS) (4-VOTES)

SUBJECT

Recommendation to approve interim ordinance authority and appropriation adjustment for the Executive Office of the Board of Supervisors to provide administrative support to the Los Angeles Memorial Coliseum Commission (Coliseum Commission).

IT IS RECOMMENDED THAT YOUR BOARD:

1. Approve an interim ordinance authority for the Executive Office of the Board of Supervisors, pursuant to County Code section 6.06.020, for one (1.0) Administrative Services Manager II and one (1.0) Senior Board Specialist to enable the Executive Office to begin providing administrative support to the Los Angeles Memorial Coliseum Commission.
2. Approve an appropriation adjustment in the amount of \$ 233,000 which includes \$ 112,000 for Salaries and Employee Benefits (S&EB), and \$121,000 for Services and Supplies (S&S) to support the first nine months of the Coliseum Commission. Included in the S&S are one-time costs of \$84,000 for system upgrades. The appropriation will be fully off-set by revenue.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

At its September 11, 2013 meeting, the Coliseum Commission voted to accept the Executive Office's proposal to assume the administrative support functions of the

Coliseum Commission, no later than January 1, 2014. The following new positions are needed to assume these functions:

- 1 - Administrative Services Manager II
- 1 - Senior Board Specialist

From October 2013 through December 2013, it is estimated that 50% of the ASM II's time and 100% of the SBS's time will be needed for the initial transition phase. From January 2014 through June 2014, approximately 75% of both the ASM II's and SBS's time will be spent on the administrative support functions. The funding requested is based on these time estimates.

The recommended positions are needed to provide the administrative support functions to the Commission, including, but not limited to: preparing, reviewing and/or submitting financial and other required reports; preparing the annual operating budget of the Commission; scheduling of regular public meetings; preparing meeting agendas and minutes, and coordinating other activities and processes, as needed.

The interim ordinance authority for these two positions will be a provisional allocation to enable the Executive Office to fill the positions for the remainder of Fiscal Year 2013-2014. Justification for inclusion of funded ordinance positions for one Administrative Services Manager II and one Senior Board Specialist will be included in the Fiscal Year 2014-2015.

IMPLEMENTATION OF STRATEGIC PLAN GOALS

The recommended actions are consistent with principles of the countywide Strategic Plan Goal 1: Operational Effectiveness.

FISCAL IMPACT/FINANCING

The appropriation adjustment for FY 2013-14, in the amount of \$233,000, will provide spending authority for S&EB in the amount of \$112,000 and S&S in the amount of \$121,000 to support the first nine months of the Coliseum Commission. The appropriation will be fully off-set by revenue.

Beginning in FY 2014-2015, and annually thereafter, the costs will be reduced to \$140,500 annually. This is primarily due to the elimination of the one-time start-up costs. The annualized cost of the S&EB and S&S will be included in the FY 2014-15 Recommended Budget.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The Los Angeles Memorial Coliseum Commission is a Joint Powers Authority (JPA) established under a management agreement between: 1) the State of California/Sixth District Agricultural Association; 2) the County of Los Angeles; and 3) the City of Los Angeles. In June 2013, the Commission approved amendments to the current JPA, (dated November 9, 1976, and initially dated September 25, 1945), and will submit the revised JPA to the State, County, and City for final signature shortly. The purpose of

the recent amendment is to revise the governance structure, meeting requirements and operating arrangements of the Coliseum Commission in view of the change in the level of the daily responsibilities of the Commission as a result of the Amended and Restated Lease with the University of Southern California ("USC") for the year-round management of the Coliseum and Sports Arena properties. The Amended and Restated USC-Coliseum Commission Lease became effective July 29, 2013.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of these recommendations will allow the Executive Office of the Board of Supervisors to begin providing administrative support to the Coliseum Commission.

Respectfully submitted,

SACHI A. HAMAI
Executive Officer, Board of Supervisors

SAH:km

Attachment

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



RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

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

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

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

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

- Developing and maintaining the Countywide Information Security Strategy Plan; ~~for the County~~
- Chairing the Information Security Steering Committee (ISSC);
- Providing ~~information~~ County IT security-related technical, regulatory, and policy leadership;
- Facilitating the implementation of County ~~information~~ IT security policies;
- Coordinating ~~information~~ County IT security efforts across ~~departmental lines~~ 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 policies;
- ~~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 approval by the Board of Supervisors. County departments requesting exceptions should shall provide such

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

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.

DataInformation 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, antispysware 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 thea

computing device.

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

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

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

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

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

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

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

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

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

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

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

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

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

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

POLICY

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

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

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

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

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

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

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

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

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

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

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

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

Definition Reference

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

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

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

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

Compliance

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

Policy Exceptions

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

Board of Supervisors Policy No. 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 encompasses information gathering, analysis, and determination of security vulnerabilities within the County IT resources, including without limitation, County's hardware and software environments, and IT information technology (I/T) business business practices.

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

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

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

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

Definition Reference

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

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

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

Compliance

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

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

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

REFERENCE

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

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

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

POLICY

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

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

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

This Policy is applicable to all County IT users.

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

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

- Properly complete the annual Chief Information Office’s Business Automation Planning (BAP) security questionnaire; 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 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:
6.109	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 to OCI. These incidents can be reported using an on-line form found at www.lacountyfraud.org. Examples of these incidents include:

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

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 approved by the Board of Supervisors. County departments requesting exceptions shall should provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County department, initiatives, actions, and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall will review such requests, confer with the

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007
Reissue Date:

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



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: