WILLIAM T FUJIOKA
Chief Executive Officer

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

**DATE:** July 11, 2013
**TIME:** 1:00 p.m.
**LOCATION:** Kenneth Hahn Hall of Administration, Room 830

## AGENDA

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

1. Call to order – Gevork Simdjian

A) **Board Letter – APPROVAL OF AMENDMENT TO SUPPLY CHAIN PROCUREMENT AND DATA MANAGEMENT SERVICES AGREEMENT WITH GLOBAL HEALTHCARE EXCHANGE LLC**
Health Services/CIO – Mitchell H. Katz and Richard Sanchez or designee(s)

B) **Board Letter – Formation of Joint Powers Authority for Redevelopment Area Refunding Program**
TTC – Mark Saladino or designee

C) **Review of IT Policies (6.100 thru 6.112)**
CIO – Richard Sanchez or designee

D) **Upcoming IT Items**
CIO – Richard Sanchez or designee

2. Public Comment

**NOTICE OF CLOSED SESSION**

CS-1 Personnel Issue Discussion

3. Adjournment

July 30, 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 AMENDMENT THREE TO SUPPLY CHAIN PROCUREMENT AND DATA MANAGEMENT SERVICES AGREEMENT NO. H-704447 WITH GLOBAL HEALTHCARE EXCHANGE LLC**
**(ALL SUPERVISORIAL DISTRICTS)**
**(3 VOTES)**

CIO RECOMMENDATION: APPROVE [×]

## SUBJECT

Request approval of an Amendment to the existing Agreement with Global HealthCare Exchange LLC for supply chain procurement and data management services at Department of Health Services facilities to amend the Statement of Work and to increase the maximum agreement sum by $309,000.

IT IS RECOMMENDED THAT THE BOARD:

Authorize the Director of Health Services (Director), or his designee, to execute Amendment Three to Agreement H-704447 with Global HealthCare Exchange LLC (GHX), for supply chain procurement and data management services, effective upon Board approval to amend the Statement of Work for additional services and increase the agreement sum by $309,000 for a revised maximum agreement sum of $2,121,765 with no change to the previously approved amount for the optional six month-to-month extension period for a maximum agreement sum of $2,243,815, subject to review and approval by County Counsel.

## PURPOSE/JUSTIFICATION OF RECOMMENDED ACTIONS

Approval of the recommendation will authorize the Director, or his designee, to execute an Amendment, substantially similar to Exhibit I, to add additional post-implementation development services, including post-implementation custom programming for data conversion, across all Department of Health Services (DHS or Department) facilities to integrate GHX Procurement Suite with the Countywide eCAPS eProcurement and eInventory systems.

The recommended Amendment with GHX will provide customized programming to enable DHS to fully integrate GHX Procurement Suite with Countywide eCAPS eProcurement and eInventory systems; and to streamline processing the Department's high volume of invoices and purchase orders through the system. This will be achieved by standardizing financial coding for all Department purchase order transactions to meet County and DHS requirements and by making other necessary customizations to GHX Procurement Suite. Moreover, the Amendment will allow DHS to maximize supply chain automation, ensure compliance by implementing controls and standards, and provide the Department with the necessary data to make data-driven decisions with regard to effectively managing the supply chain process.

**Implementation of Strategic Plan Goals**

The recommended actions support Goal 1, Operational Effectiveness and Goal 3, Integrated Services Delivery of the County's Strategic Plan.

**FISCAL IMPACT/FINANCING**

With this Amendment, the County's maximum agreement sum will be increased by $309,000 from $1,812,765 to $2,121,765 for the agreement period ending June 30, 2015.

Funding is included in DHS' Fiscal Year 2013-2014 Adopted Budget, and will be requested in future fiscal years.

All of these costs will be offset by Patron Equity Credits (PECs). DHS has accrued PECs, which are available to DHS to offset other charges, through the Department's participation in University HealthSystem Consortium's (UHC) group purchasing organization (GPO). These credits are awarded to DHS based on its purchase of commodities through UHC agreements and can be used to purchase services from GHX. DHS will utilize PECs to fund these services. After UHC rebates these PECs to DHS, DHS will use these credits to pay for the additional services.

**FACTS AND PROVISIONS/LEGAL REQUIREMENTS**

GHX is a Business Exchange made up of healthcare providers and healthcare product vendors. UHC members, including DHS, are the primary members of GHX. GHX provides current and up-to-date procurement data on medical supplies and to assist members with maintaining a uniform and an efficient supply formulary for medical and surgical supplies. GHX is the only company in the United States to specialize in healthcare supply chain data management and is currently integrated with all major GPOs, including Novation.

DHS has maintained membership in UHC, a not-for-profit member alliance of approximately 118 academic medical centers and its medical commodity contracting

division, Novation, since 1997. As a UHC member, DHS has the ability to access UHC agreements as an alternative to conducting competitive solicitations.

As a member of UHC, the Department benefits from group discounts for all medical supplies covered under UHC-established vendor contracts. Consequently, DHS benefits from economies of scale. DHS utilizes GHX's supply chain procurement and data management services to increase its savings and more effectively leverage its purchasing power.

On September 21, 2010, the Board approved Agreement H-704447 with GHX for supply chain procurement and data management services for an initial term through June 30, 2013 with one two-year extension and six month-to-month extensions. These services maximize DHS' supply chain results with the following: development of a standardized supply formulary; implementation of controls to ensure compliance with the established formulary; reconciliation and cleansing of purchasing data for consistency and completeness; and hosting of established UHC supplier agreements.

On January 1, 2012, the Department executed Amendment One to exercise its delegated authority to increase the County's total agreement sum by 10 percent, an additional $120,415, to address additional service needs. On May 22, 2013, the Department executed Amendment Two to exercise its delegated authority to extend the Agreement term to June 30, 2015.

County Counsel has reviewed and approved the Amendment (Exhibit I) as to form. The Chief Information Officer concurs with the Department's recommendation and the CIO Analysis is attached.

## CONTRACTING PROCESS

Under the current Agreement, GHX implemented its proprietary supply chain procurement and data management software and services. Additional modifications, interfaces, and new reports are necessary and exceed the current delegation of authority for custom programming in the GHX Agreement. It is not feasible to have another vendor provide these services; therefore, DHS did not conduct a solicitation.

## IMPACT ON CURRENT SERVICES (OR PROJECTS)

Approval of the recommendation will enable the Department to continue its post-implementation of supply chain automation at all DHS facilities and to provide DHS with the necessary software to develop a standardized supply formulary across all DHS facilities.

DRAFT

Respectfully submitted,

Mitchell H. Katz, M.D.
Director

Reviewed by:

Richard Sanchez
Chief Information Officer

MHK:jl

Enclosures (2)

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

DRAFT

ATTACHMENT

RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

Office of the CIO

# CIO Analysis

| NUMBER: | DATE: |
|---|---|
| CA 13-12 | 6/4/2013 |

SUBJECT:

**APPROVAL OF AMENDMENT THREE TO SUPPLY CHAIN PROCUREMENT AND DATA MANAGEMENT SERVICES AGREEMENT WITH GLOBAL HEALTHCARE EXCHANGE LLC**

RECOMMENDATION:

☒ Approve ☐ Approve with Modification ☐ Disapprove

CONTRACT TYPE:

☐ New Contract ☐ Sole Source
☒ Amendment to Contract #: H-704447 ☐ Other: Describe contract type.

CONTRACT COMPONENTS:

☐ Software ☐ Hardware
☐ Telecommunications ☒ Professional Services

SUMMARY:

Department Executive Sponsor: **Mitchell H. Katz, M.D.**

Description: Authorize the Director of Health Services (Director), or his designee, to execute Amendment No. Three to Agreement H-704447 with Global HealthCare Exchange LLC (GHX), for supply chain procurement and data management services, effective upon execution to amend the Statement of Work for additional services and increase the agreement sum by $309,000 for a revised maximum agreement sum of $2,121,765 with no change for the previously approved amount for the optional six month-to-month extension period for a maximum agreement sum of $2,243,815.

Contract Amount: **$309,000**

Funding Source: **DHS Operating Budget Fiscal Year 2013-14 ***

☐ Legislative or Regulatory Mandate ☒ Subvented/Grant Funded: **100 % ***

- See footnote in the Financial Analysis section.

| ***Strategic and Business Analysis*** | PROJECT GOALS AND OBJECTIVES: To align with the Department's goal to reduce cost and improve efficiency of ordering crucial medical supplies using a standard formulary. GHX has been instrumental in streamlining the supply chain process for DHS and its interface into the County eCAPS system. This Amendment will standardize financial coding for all Department purchase order transactions to meet County and DHS requirements and by making other necessary customizations to GHX' Procurement Suite, including the creation of necessary technical interfaces, product code changes, and reports. |
|---|---|

BUSINESS DRIVERS:

The key business drivers for the project are:

1. **Operational efficiency**: The solution uses a standard formulary and a single system to order medical and non-medical supplies; this has already improved the efficiency of operation. Additionally, GHX interfaces with the County procurement system eCAPS which will further improve operational efficiencies.

2. **Cost Reduction:** This solution also reduces costs by using standardized formulary with discounted prices.

PROJECT ORGANIZATION:

Gary D. McMann, Chief of Supply Chain Network, is the Project Executive Sponsor. Mauricio Aguilar, Manager of Supply Chain Information Systems, is the Project Director.

PERFORMANCE METRICS:

This system enhancements will assist DHS to increase its savings and more effectively leverage its purchasing power. DHS will be able to maximize supply chain automation, ensure compliance by implementing controls and standards, and provide the necessary data to make data-driven decisions to streamline supply chain process.

STRATEGIC AND BUSINESS ALIGNMENT:

The project supports the following County Strategic Plan goal: Operational Effectiveness and Goal 3, Integrated Services Delivery of the County's Strategic Plan.

PROJECT APPROACH:

The vendor will perform the agreed upon application modifications to GHX Procurement Suite and the GHX' Transfer Engine. Mauricio Aguilar, Manager of Supply Chain Information Systems will be the Project Manager who will provide the appropriate project planning and guidance to ensure the application modifications are fully tested before user acceptance.

ALTERNATIVES ANALYZED:

This is an Amendment to an existing Agreement. No alternative was considered.

| | |
|---|---|
| ***Technical Analysis*** | ANALYSIS OF PROPOSED IT SOLUTION:<br>The GHX/eCAPS Integration Interface is based on numerous crosswalk tables that are not providing the financial data required by DHS Finance to justify reimbursements for medical supplies. This Amendment will allow changes to be made to the GHX suite of applications to create additional fields to store required financial data by eliminating the need for the crosswalk tables.<br>The service details are described in the Statement of Work (SOW). It covers a new interface to load the Procurement Master table data from eCAPS into GHX' transfer engine. The transfer engine is also modified to ensure proper coding of each item. A new report will be created for items that are not coded and this validation will eliminate downstream issues. Other modifications will also be made to improve data integrity and streamline navigation. |
| ***Financial Analysis*** | BUDGET:<br>**Contract costs:**<br><br>One-time costs: (for Amendment Three)<br>Services..... $309,000<br>**Total one-time costs: $309,000 ***<br><br>Previous contract cost: $1,812,765.00 (includes Amendments One & Two)<br><br>**Total Contract sum: $2,121,765**<br>**Optional cost: (6 months max): $122,050**<br>**Total cost (maximum): $2,243,815**<br><br>Other County costs: N/A<br><br>*DHS budgeted the annual amount because the anticipated credits cannot be calculated. However, based on the volume of purchases, they are receiving 100% credit from the University HealthSystem Consortium (UHC) group. This is part of their budgetary and financing process. |
| ***Risk Analysis*** | RISK MITIGATION:<br>1. DHS needs a thorough requirements analysis document to capture all the code changes. Effective project governance is also critical.<br>2. The Chief Information Security Officer (CISO) has reviewed the Amendment and did not identify any IT security or privacy related issues. |

DRAFT

| | | |
|---|---|---|
| ***CIO Approval*** | PREPARED BY: | |
| | Sanmay Mukhopadhyay, Sr. Associate CIO | Date |
| | APPROVED: | |
| | Richard Sanchez, County CIO | Date |

Please contact the Office of the CIO (213.253.5600 or info@cio.lacounty.gov) for questions concerning this CIO Analysis. This document is also available online at http://ciointranet.lacounty.gov/

DRAFT

August 6, 2013

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

The Honorable Board of Directors
Los Angeles County Public Works Financing Authority
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, CA 90012

Dear Supervisors:

**FORMATION OF THE COUNTY OF LOS ANGELES**
**REDEVELOPMENT REFUNDING AUTHORITY**
**(ALL DISTRICTS) (3 VOTES)**

**SUBJECT**

The Treasurer and Tax Collector is seeking approval of a Joint Exercise of Powers Agreement between the County of Los Angeles and the Los Angeles County Public Works Financing Authority to establish the County of Los Angeles Redevelopment Refunding Authority for the purpose of refunding various debt obligations of the former redevelopment agencies within Los Angeles County.

**IT IS RECOMMENDED THAT YOUR BOARD:**

Adopt the resolution approving a Joint Exercise of Powers Agreement (the "Joint Powers Agreement") between the County of Los Angeles and the Los Angeles County Public Works Financing Authority (the "PWFA") to establish the County of Los Angeles Redevelopment Refunding Authority (the "Authority").

**IT IS RECOMMENDED THAT YOUR BOARD, ACTING AS THE BOARD OF DIRECTORS OF THE LOS ANGELES COUNTY PUBLIC WORKS FINANCING AUTHORITY:**

Adopt the resolution approving the Joint Powers Agreement between the County of Los Angeles and the PWFA to establish the Authority.

**PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION**

California Assembly Bill No. 26 (First Extraordinary Session) ("AB1X 26"), which was adopted on June 29, 2011, dissolved all redevelopment agencies ("RDAs") in the State of California as of February 1, 2012, and designated "successor agencies" and "oversight boards" to satisfy the "enforceable obligations" of the former redevelopment agencies. Included among the enforceable obligations contemplated by AB1X 26 were the numerous tax allocation bonds issued by the former RDAs throughout the State.

In Los Angeles County, it is estimated that the 71 former RDAs issued in excess of 300 series of tax allocation bonds with a par amount of more than $3.5 billion currently outstanding. The majority of these bonds carry interest rates that significantly exceed the rates that could be obtained in the current bond market. Assembly Bill 1484 ("AB 1484"), which was enacted on June 27, 2012, provides a mechanism for successor agencies to refund outstanding bond obligations for the purpose of debt service savings. In both the County and the State, successor agencies are typically the city that originally sponsored the formation of the RDA. As a result, these cities are given the opportunity to initiate tax allocation bond refundings and generate savings for the benefit of the local taxing agencies, including the County, that receive a share of the property tax increment.

In January 2013, the Treasurer and Tax Collector informed your Board of the Redevelopment Bond Refunding Program (the "Program") that had been initiated in order to refinance existing bond obligations of the RDAs in Los Angeles County. One of the main objectives for establishing the Program was to minimize the amount of time and effort required of the successor agencies, while also providing significant economies of scale through reduced costs of issuance and lower interest rates.

The Program is designed to provide multiple refunding opportunities over the next several years with the inaugural issuance in 2013 focused on refunding only a portion of the outstanding tax allocation bonds. Numerous successor agencies have expressed interest in joining the Program and are expected to participate in either the 2013 refunding or perhaps join in subsequent years. As of the date of this letter, six (6) successor agencies (Alhambra, Claremont, [Covina], Monterey Park, [South Gate] and West Hollywood) have opted to participate in the Program and issue 2013 tax allocation refunding bonds through the County. These six successor agencies have [15] outstanding series of bonds that qualify for refunding, which will produce over [$16.7] million in gross debt service savings, or more than [$11] million in net present value savings. The 2013 tax allocation refunding bonds are currently expected to be issued in one or more series in a principal amount of no more than [$140,000,000].

The initial issuance of refunding bonds is expected to be sold through a "pooled" financing structure that is common to California municipal finance and which requires the use of a joint powers authority ("JPA"). Specifically, each of the six successor agencies will issue its own

series of refunding bonds, which will then be pooled together into one or more financings and sold to the capital markets through the Authority that is to be established by your Board. In consultation with both County Counsel and the financing team selected for this financing, the Treasurer and Tax Collector has concluded that the most advantageous manner to carry out the issuance of the bonds is for the County to form a new JPA to facilitate the issuance of the pooled bonds. It is therefore recommended that the County and the PWFA form a joint exercise of powers entity to be known as the County of Los Angeles Redevelopment Refunding Authority by agreement pursuant to Articles 1 through 4, Chapter 5, Division 7, Title 1 of the California Government Code (commencing with Section 6500), as amended. Unlike the existing PWFA, which is commonly used in the issuance of County debt obligations backed by the General Fund, the Authority will be utilized solely for the purpose of refunding debt of the former RDAs and will not serve as an issuer of County debt. The formation of a new, redevelopment-specific JPA to issue the refunding bonds will assist potential investors and credit rating agencies in differentiating between Agency debt and those County obligations issued by the PWFA. This is relevant mostly in relation to County's lease revenue bonds, whose "AA-" rating from Standard & Poor's is notably higher than the "BBB" to "A" ratings that we anticipate for the tax allocation refunding bonds.

**Implementation of Strategic Plan Goals**

This action supports the County's Strategic Plan Goal #1: Operational Effectiveness through collaborative actions among the County and the public and private sector to provide investment in public and private benefit infrastructure within the County.

**FISCAL IMPACT/FINANCING**

There will be no fiscal impact to the County budget as a result of forming the JPA. The issuance of refunding bonds will provide additional general fund revenues that can be utilized for other County purposes.

**FACTS AND PROVISIONS/LEGAL REQUIREMENTS**

The legal authority to approve the JPA and to establish the Authority is derived pursuant to Articles 1 through 4, Chapter 5, Division 7, Title 1 of the California Government Code (commencing with Section 6500), as amended. The attached resolutions and Joint Powers Agreement have been reviewed and approved by County Counsel, with consultation provided by outside bond counsel.

To assist the County with the establishment of the Program, the Treasurer and Tax Collector has assembled a team of professionals with extensive experience in the area of redevelopment financing. Based on the results of a formal solicitation process, De La Rosa & Co. was selected to be the senior managing underwriter, and Citigroup as co-senior manager. KNN Public Finance has been selected as financial advisor, and Orrick, Herrington & Sutcliffe was chosen as bond counsel.

DRAFT

**IMPACT ON CURRENT SERVICES (OR PROJECTS)**

Not applicable.

**CONCLUSION**

Upon approval, it is requested that the Executive Officer-Clerk of the Board of Supervisors return two originally executed copies of the adopted resolution to the Treasurer and Tax Collector (Office of Public Finance).

Respectfully submitted,

MARK J. SALADINO
Treasurer and Tax Collector

Attachments

c: Executive Office, Board of Supervisors
Auditor-Controller
Chief Executive Officer
County Counsel
Orrick, Herrington & Sutcliffe LLP

DRAFT

# COUNTY OF LOS ANGELES

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

RICHARD SANCHEZ
CHIEF INFORMATION OFFICER

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


July 27, 2013

To: Audit Committee

From: Richard Sanchez
Chief Information Officer

**REVIEW OF BOARD POLICIES 6.100 - 6.112 - INFORMATION SECURITY**

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

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

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

RS:RP:pg

Attachments

c: Chief Executive Officer
Executive Officer, Board of Supervisors

DRAFT

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

## Summary of Revisions

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

DRAFT

## Summary of Revisions

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

DRAFT

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

## REFERENCE

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

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

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

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

DRAFT

- ~~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;

DRAFT

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

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

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

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

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

DRAFT

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

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

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

**General**

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

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

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

## RESPONSIBILITIES

**~~Departments, Commissions, Board and Offices~~**

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

DRAFT

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

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

**Chief Information Office (CIO)**

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

**Chief Information Security Officer (CISO)**

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

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

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

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

**County Department IT Management / Departmental Chief Information Officer**

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

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

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

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

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

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

**Departmental Information Security Officer (DISO)**

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

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

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

**~~Employees and Other Authorized Users~~ County Users**

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

**Information Security Steering Committee ~~(ISSC)~~**

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

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

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

**Compliance**

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

DRAFT

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

## RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

## DATE ISSUED/SUNSET DATE

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

**Reissue Date:** **Sunset Review Date:**

DRAFT

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

## REFERENCE

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

DRAFT

~~Acceptable Use Agreement (Attached)~~

## POLICY

---

### General

This policy is applicable to all County IT users.

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

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

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

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

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

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

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

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

DRAFT

~~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.)~~

DRAFT

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

**Access Control**

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

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

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

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

**Authentication**

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

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

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

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

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

DRAFT

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

**~~Data~~Information Integrity**

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

**Accessing County IT ~~Technology~~ Resources Remotely**

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

**Privacy**

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

**Confidentiality**

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

**Definition Reference**

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

DRAFT

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

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

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

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

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

**Compliance**

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

**Policy Exceptions**

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

~~(See Acceptable Use Agreement)~~

## RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

## DATE ISSUED/SUNSET DATE

**Issue Date: July 13, 2004**

**Sunset Date: July 13, 2008**

**Reissue Date:**

**Sunset Review Date:**

DRAFT

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

## ANNUAL

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

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

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

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

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

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

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

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

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

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

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

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

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

9. Computer virus and other malicious devices ~~code:~~ I shall ~~will~~ not intentionally introduce any malicious device (e.g., computer virus, spyware, and ~~worms or~~ malicious code), into any County IT resources. ~~computer, network, system or data.~~ I shall not use County IT resources to intentionally introduce any malicious device into any County IT resources or any non-County IT systems or networks. I shall ~~will~~ not disable, modify, or delete computer security software (e.g., antivirus software, antispyware software, firewall software, and host intrusion prevention software) on County IT resources. I shall notify the County Department's Help Desk and/or DISO as soon as any item of County IT resources is suspected of being compromised by a

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

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

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

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

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

14. Public forums ~~Internet~~: I shall not use County IT resources to create, exchange, publish, distribute, or disclose in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) without understanding the potential risk. ~~I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services may be filtered but in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be inadvertently exposed to such offensive materials. I understand that my Internet~~

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:**

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



DRAFT

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

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

DRAFT

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

## REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

## POLICY

This policy is applicable to all County IT users.

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

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

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

DRAFT

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~~

DRAFT

~~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~~.

DRAFT

## Policy Exceptions

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

**RESPONSIBLE DEPARTMENT**

Chief Information Office ~~(CIO)~~

**DATE ISSUED/SUNSET DATE**

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

**Reissue Date:** **Sunset Review Date:**

DRAFT

Los Angeles County
# BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

## REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

## POLICY

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

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

DRAFT

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

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

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

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

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

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

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

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

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

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

## Definition Reference

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

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

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

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

## Compliance

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

## Policy Exceptions

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

## RESPONSIBLE DEPARTMENT

---

Chief Information Office ~~(CIO)~~

DRAFT

## DATE ISSUED/SUNSET DATE

**Issue Date: July 13, 2004**

**Sunset Date: July 13, 2008**

**Reissue Date:**

**Sunset Review Date:**

DRAFT

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

## REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

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

## POLICY

DRAFT

This policy is applicable to all County IT users.

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

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

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

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

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

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

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

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

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

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

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

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

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

**Definition Reference**

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

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

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

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

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

**Compliance**

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

**Policy Exceptions**

DRAFT

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:**

DRAFT

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

DRAFT

## POLICY

---

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

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

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

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

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

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

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

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

DRAFT

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

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

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

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

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

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

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

DRAFT

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

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

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

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

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

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

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

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

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

DRAFT

- ~~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.~~

DRAFT

## Definition Reference

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

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

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

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

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

## Compliance

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

## Policy Exceptions

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

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

## RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

## DATE ISSUED/SUNSET DATE

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

**Reissue Date:** **Sunset Review Date:**

DRAFT

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

## REFERENCE

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

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.

DRAFT

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~~

DRAFT

~~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**

DRAFT

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:**

DRAFT

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 ifentifying 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.

DRAFT

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

DRAFT

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

**Policy Exceptions**

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

**RESPONSIBLE DEPARTMENT**

Chief Information Office ~~(CIO)~~

**DATE ISSUED/SUNSET DATE**

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

**Reissue Date:** **Sunset Review Date:**

DRAFT

Los Angeles County
# BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

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

## REFERENCE

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

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

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

## POLICY

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

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

DRAFT

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

This policy is applicable to all County IT users.

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

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

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

**Definition Reference**

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

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

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

**Compliance**

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

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

DRAFT

other actions as well as both civil and criminal penalties.

**Policy Exceptions**

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

## RESPONSIBLE DEPARTMENT

Chief Information Office ~~(CIO)~~

## DATE ISSUED/SUNSET DATE

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

**Reissue Date:** **Sunset Review Date:**

DRAFT

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

DRAFT

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 a~~n~~ County IT ~~related~~ security incident occurs. For purposes of this coordination, the CISO has the responsibility for the CIO. The ~~County~~ Chief HIPAA Privacy Officer ~~(HPO)~~ and the Office of County Investigations (OCI) have respective

responsibilities for the Auditor-Controller.

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

**Chief Information Security Officer (CISO)**

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

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

**Chief HIPAA Privacy Officer (CHPO)**

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

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

**Office of County Investigations (OCI)**

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

- System breaches from internal or external sources

DRAFT

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

**Chief Information Office (CIO)**

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

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

**Definition Reference**

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

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

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

DRAFT

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

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

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

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

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

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

**Compliance**

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

**Policy Exceptions**

There are no exceptions to this policy.

**RESPONSIBLE DEPARTMENT**

Chief Information Office

## DATE ISSUED/SUNSET DATE

**Issue Date: May 8, 2007**
**Reissue Date:**

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

DRAFT

Los Angeles County
# BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

## REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

Health Insurance Portability and Accountability Act (HIPAA) OF 1996

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

DRAFT

## 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~~

DRAFT

~~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

DRAFT

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.

DRAFT

## RESPONSIBLE DEPARTMENT

Chief Information Office

## DATE ISSUED/SUNSET DATE

**Issue Date: May 8, 2007**

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

**Reissue Date:**

**Sunset Review Date:**

DRAFT

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

**Department Name** _____

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

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

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

## Portable Computing Device Description:

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

Device serial number: _____

Property number (if County property): _____

Name of encryption software installed: _____

DRAFT

Operating system: _____

## Information Being Placed on the Portable Computing Device:

Purpose of placement: _____

Application system name (if applicable): _____

Personal and/or confidential information fields: _____

_____

_____

_____

_____

_____

## User Agreement and Acknowledgement:

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

Name: _____ Date: _____

Signature: _____

## Department Approval:

Print Name: _____ Title: _____

Signature: _____

DRAFT

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

## REFERENCE

May 8, 1007, Board Order No. 26 – Board of Supervisors – Information Security Policies

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

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

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

## POLICY

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

DRAFT

~~employment with the County.~~

This policy is applicable to all County IT users.

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

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

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

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

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

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

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

Information security awareness training shall be provided to County IT users

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

**Definition Reference**

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

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

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

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

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

**Compliance**

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

**Policy Exceptions**

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

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

## RESPONSIBLE DEPARTMENT

Chief Information Office

## DATE ISSUED/SUNSET DATE

**Issue Date: May 8, 2007**
**Reissue Date:**

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

DRAFT

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

## PURPOSE

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

## REFERENCE

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

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

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

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

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

## POLICY

This policy is applicable to all County IT users.

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

DRAFT

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

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

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

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

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

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

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

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

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

• Computing device sent to salvage

• Computing device destroyed

• Computing device donated to a non-County organization

**Definition Reference**

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

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

DRAFT

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:**

DRAFT

# Board IT Agenda Items

| Department | Board IT Agenda Item | Description | Amount | CEO Cluster | New Term | Planned Hearing Date |
|---|---|---|---|---|---|---|
| DHS | Authorize Purchase of Hardware for the Department of Health Services Data Center to support the Picture Archiving and Communication System (PACS) | Authorize Purchase of Hardware for the Department of Health Services Data Center to support the Picture Archiving and Communication System (PACS).<br><br>**Funding Source: DHS FY 2013-14 Operating Budget**<br>**Existing Agreement: N/A** | $430,000 | Health & Mental Health Services | 3 years maintenance | 7/9/2013 |
| DHS | Amendment of the GHX Supply Chain Management system contract for enhancements . | The current DHS GHX system needs to be modified to create interfaces and reports.<br><br>**Funding Source: DHS FY 2013-14 Operating Budget**<br>**Existing Agreement: 70447** | $309,000 | Health & Mental Health Services | 2 years | 7/30/2013 |
| FIRE | Execute Work Order Under the County's IBM Master Services Agreement No. 75869 for Fire Facility Management System | Work Order for implementation services to implement Maximo Facilities Management System.<br><br>**Funding Source: Fire FY 2013-14 Operating Budget**<br>**Existing Agreement: 75869** | $398,409 | Public Safety | TBD | 7/30/2013 |
| DPW | El Segundo Area Intelligent Transportation System Project Amendment Number Four to Agreement PW 12694 for Software and Services | This action is to approve and authorize the Director, or her designee to execute Amendment Number 4 to Software and Services Agreement PW 12694 with Iteris, Inc., for the El Segundo Area Intelligent Transportation System Project to extend the agreement term for two years to provide for continued services and maintenance of the system with no increase in the total agreement sum. This action will also delegate authority to the Director of Public Works or her designee to execute future no cost amendments, if necessary, to further extend the term for up to two additional two-year terms.<br><br>**Funding Source: N/A (time-only Amendment)**<br>**Existing Agreement: PW 12694** | NTE $6,820,782 (approx. $3.9M spent to date) **No increase requested** | Community & Municipal Services | 2 yr. extension + up to two additional 2 yr. (delegated to Dir, DPW) | 8/6/2013 |

| Department | Board IT Agenda Item | Description | Amount | CEO Cluster | New Term | Planned Hearing Date |
|---|---|---|---|---|---|---|
| DHS | Approval of Amendment to Equipment Maintenance and Repair Services Agreement with Parata Systems and Talyst, Inc. | Approval of Amendment 2 to Equipment Maintenance and Repair Services Agreement with Parata Systems, LLC to add resources and extend the term.<br>Approval of Amendment 1 to agreement with Talyst, Inc., for equipment maintenance and repair services of the automated medication management systems add resources and extend the term.<br><br>**Funding Source: DHS FY 2013-14 Operating Budget**<br>**Existing Agreement: H702976** | $1.39M (Parata) + $1.17M (Talyst) | Health & Mental Health Services | TBD | 8/6/2013 |
| DHS | Agreement for Web-based eConsult System and related services between County and SafetyNetConnect | Agreement for development of eConsult software for DHS ACN and SafetyNetConnect.<br><br>**Funding Source: DHS FY 2012-13 Operating Budget**<br>**Existing Agreement: N/A** | $4.8M | Health & Mental Health Services | TBD | 8/6/2013 |
| CIO/CEO/DHS/ DMH & DCFS | Countywide Master Data Management (CWMDM) | Implement a Master Data Management solution for the entire County, to include:<br><br>1. Development and maintenance of a catalog of enterprise data objects. (Data entities, Authoritative sources, Attributes, Values, Access control and policies).<br>2. Development and maintenance of a catalog of existing system interfaces.<br>3. Development of policies for enterprise information management.<br>4. Building of an Enabling Infrastructure (shared service) for enterprise information management, including Master Data Management; Enterprise Messaging and Service Bus; and Data Analytics.<br><br>**Funding Source: TBD**<br>**Existing Agreement: N/A** | TBD | Operations | TBD | 9/17/2013 |
| CIO | Los Angeles Region Imagery Acquisition Consortium (LAR-IAC) 4 Agreement | Agreement to acquire digital aerial data for County and participating agencies.<br><br>**Funding Sources: County Dept Operating Budgets and Participating Cities & Agencies**<br>**Existing Agreement: LAR-IAC 3** | $4M (Est.) | Operations | 3 years, with 9 optional years | 10/1/2013 |

| Department | Board IT Agenda Item | Description | Amount | CEO Cluster | New Term | Planned Hearing Date |
|---|---|---|---|---|---|---|
| DCFS | Contract with SAS, Inc. | SAS, Inc. to provide consultants to pilot the Advanced Analytics Data Mining project to be used to estimate children at risk and to improve child welfare operations within the department.The proposed pilot would involve DCFS providing to SAS, Inc. three years of de-identified historical data from the existing data structures. SAS, Inc., would link data across the systems and apply its analytic data mining capabilities to identify when certain cases should have merited closer attention.<br><br>**Approx. Board Date: TBD**<br>**Funding Source: DCFS FY 2013-14 Operating Budget (NCC)**<br>**Existing Agreement: N/A** | $99,000 | Children & Families Well-being | 1 year | |
| CIO/LASD/FIRE/ OEM | Extension of AlertLA Agreement with 21st Century Communications | 1. Request one-year extention for AlertLA Mass Notification System with 21st Century Communications System.<br>2. Develop new RFP<br><br>**Approx. Board Date: TBD**<br>**Funding Source: ITF**<br>**Existing Agreement: 76945** | N/A | Operations, Public Safety | 1 year | |
| LASD | Multimodal Biometric Identification System (MBIS) | Development of an automated biometric identification system to replace current Cogent system.<br><br>**Approx. Board Date: TBD**<br>**Funding Source: RAND Board**<br>**Existing Agreement: N/A** | TBD | Public Safety | TBD | |

| Department | Board IT Agenda Item | Description | Amount | CEO Cluster | New Term | Planned Hearing Date |
|---|---|---|---|---|---|---|
| DPW | Contract for Alamitos Barrier Project and Dominguez Gap Barrier Project Telemetry System Maintenance Services | Contract for Alamitos Barrier Project & Dominguez Gap Barrier Project Telemetry System Maintenance Services.<br><br>• Background: The Dominguez Gap and Alamitos Barriers are seawater barriers that are designed to inject freshwater into underground aquifers to create protective pressure ridges and prevent seawater from contaminating groundwater supplies. Portions of the Dominguez Gap and Alamitos Barriers are outfitted with Supervisory Control and Data Acquisition (SCADA) systems that enable operators to remotely monitor conditions and control equipment through COTS user interfaces. Other portions of the barrier systems are manually operated.<br><br>• Scope: Inspection, maintenance, as-needed repairs, including software configuration and re-programming, and the integration of the manual segments into the automated systems. Note: the Dominguez Gap and Alamitos Barrier systems will remain separate.<br><br>**Approx. Board Date: TBD**<br>**Funding Source: Flood Fund (No County General funds)**<br>**Existing Agreement: N/A** | $600,000 per year for up to 5 years | Community & Municipal Services | 1 year, with four 1-year option extensions | |
| CIO | Use of ITF for Enterprise IT Security and Privacy Awareness Training Software | Use of ITF to acquire and implement the enterprise IT Security and Privacy Awareness training content for use in the County's Learning Net.<br><br>**Approx. Board Date: TBD**<br>**Funding Source: ITF**<br>**Existing Agreement: N/A** | $240,000 | Operations | N/A | |