County of Los Angeles
CHIEF EXECUTIVE OFFICE
OPERATIONS CLUSTER

WILLIAM T FUJIOKA
Chief Executive Officer

DATE: August 28, 2014
TIME: 1:00 p.m.
LOCATION: Kenneth Hahn Hall of Administration, Room 830

AGENDA

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

1. Call to order – Santos H. Kreimann

A) **Board Letter - ADOPT RESOLUTION AUTHORIZING THE ASSESSOR TO APPLY FOR THE STATE-COUNTY ASSESSORS PARTNERSHIP AGREEMENT PROGRAM**
Assessor – Sharon Moller or designee

B) **Approval of Revisions to Board IT Security Policies 6.100 – 6.112**
CIO – Richard Sanchez or designee

2. Public Comment

3. Adjournment

DRAFT

September 9, 2014

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

Dear Supervisors:

ADOPT RESOLUTION
AUTHORIZING THE ASSESSOR TO APPLY FOR THE STATE-COUNTY ASSESSORS PARTNERSHIP AGREEMENT PROGRAM
(All Supervisorial Districts)
(3 Votes)

SUBJECT

Adopt the attached resolution as required by the State of California Revenue and Taxation Code Section 95.5 for participation in a three year State-County Assessors Partnership Agreement Program.

IT IS RECOMMENDED THAT THE BOARD:

Adopt a Resolution authorizing the Assessor, or his designee, to submit an application, in the form and manner specified by the California Department of Finance, for participation in the State-County Assessors Partnership Agreement Program.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTIONS

The State of California Budget bill (SB854), added Section 95.5 of the Revenue and Taxation Code which creates the State-County Assessors Partnership Agreement Program (SCAPAP) for the 2014-15 fiscal year through the 2016-17 fiscal year to provide for more funding for California Assessor's Offices. Section 95.5 requires county Boards of Supervisors to adopt resolutions authorizing Assessors to apply for participation in the SCAPAP. This resolution recognizes that SCAPAP is a three year program that requires a dollar-for-dollar match by counties in exchange for state funds.

In recognition that over 50% of annual property tax revenues accrue to K-14 schools and county offices of education and thereby offset the state's General Fund obligation to those entities, the state has a vested financial interest in ensuring that the county assessors have the resources necessary to fairly and efficiently administer the county property tax rolls. Fair and efficient administration includes, but is not limited to, the expeditious enrollment of properties that are newly constructed or that change ownership, the timely levying of supplemental assessments when ownership changes occur, the timely reassessment of property to reflect market values, and the defense of assessed valuations.

SCAPAP requires that each participating county shall match, on a dollar-for-dollar basis, the program funds apportioned to their county assessor's office. SCAPAP funds provided to county assessors shall be used to supplement, and not supplant, existing funding. Base staffing and funding levels shall be calculated as of June 30, 2014, unless otherwise authorized be the Department of Finance.

IMPLMENTATION OF STRATEGIC PLAN GOALS

The recommended action supports Goal 1, Operational Effectiveness of the County's Strategic Plan.

FISCAL IMPACT/FINANCING

The total maximum obligation for the SCAPAP is $1,875,000 annually as a dollar-for-dollar match as required by Revenue and Taxation Code Section 95.5.

FACTS AND BACKGROUND

It was the intent of the California Legislature to establish a three-year pilot program limited to nine competitively selected county assessors' offices to provide county assessors with state grants to improve their ability to perform essential property tax administration duties. The success of the SCAPAP pilot program shall be determined based on whether the assessment activities funded with pilot program funds in each county have enhanced countywide equalization by properly valuing property and thereby generate property tax revenues for K-14 schools and county offices of education in an amount that is not less than the total amount of General Fund renues expended to fund the pilot program in participating county.

It is the intent of the California Legislature that the Department of Finance seek to ensure that the county applicants selected to participate in SCAPAP consist of a representative cross section of the state's county assessors' offices. Therefore, it is the

intent of the California Legislature that the Department of Finance considers factors other than revenue generating potential when reviewing applications.

PROVISIONS/LEGAL REQUIREMENTS

The Department of Finance shall review the applications and select program participants based on the strength of those applications and notify the participants of their selection no later than October 15, 2014. No later than October 22, 2014, and each October 22 thereafter while the program is operative, the Department of Finance shall instruct the office of the State Controller to remit to each participating county the appropriate sum.

County Counsel has reviewed and approved the attached

CONTRACTING PROCESS

N/A

IMPACT ON CURRENT SERVICES (OR PROJECTS)

Current services will not be impacted.

Respectfully submitted,

Sharon Moller
Interim Director

SM:GR:SH:af

Attachment

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

RESOLUTION

OF THE BOARD OF SUPERVISORS FOR THE COUNTY OF LOS ANGELES APPROVING THE APPLICATION OF STATE-COUNTY ASSESSORS' PARTNERSHIP AGREEMENT PROGRAM

WHEREAS, the California legislature has established a three-year pilot program limited to nine competitively selected county assessors' offices to quantify the benefit of providing county assessors with state grants to improve their ability to fairly and efficiently administer the county property tax rolls, and related essential duties;

WHEREAS, the State-County Assessors' Partnership Agreement Program (SCAPAP) was created to be administered by the California Department of Finance (FINANCE);

WHEREAS, all counties shall be eligible to apply to participate in SCAPAP;

WHEREAS, a maximum of two program participants shall be selected from counties of the first or second class, inclusive, as defined by Government Code sections 28022 and 28023, respectively;

WHEREAS, the selected county belonging to the first or second class is eligible to receive at least 25 percent of the amount annually appropriated for SCAPAP, not to exceed the amount of $1,875,000 annually for each fiscal year 2014-15 through 2016-17, inclusive;

WHEREAS, the selected county is required to provide matching funds to its Assessors' Office, on a dollar-for-dollar basis;

WHEREAS, SCAPAP funds provided by FINANCE and matching funds provided by county shall be used to supplement, and not supplant, existing funding to the Assessor;

WHEREAS, the county assessors' offices that elect to participate in the SCAPAP shall submit an application, in the form and manner specified by FINANCE and to transmit to FINANCE a resolution of the County Board of Supervisors that stated the county agrees to provide the Assessors' Office with matching funds, on a dollar-for-dollar, in each year that the Assessor's Office participate in the SCAPAP, no later than September 15, 2014;

WHEREAS, the Los Angeles County Assessor's Office (ASSESSOR) elects to apply to participate in the SCAPAP pursuant to Revenue and Taxation Code Section 95.5;

WHEREAS, Los Angeles County (LACO) has a population of 10 million as of January 2014 and is categorized as a county of the first class (Government Code Section 28022);

WHEREAS, LACO is eligible to apply for and receive at least 25 percent of the amount annually appropriated for SCAPAP, not to exceed $1,875,000 annually for each fiscal year 2014-15 through 2016-17, inclusive; and

WHEREAS, it is in the best interest of LACO to participate in SCAPAP because the additional property tax revenue to be generated from improved efficiency and added resources is anticipated to be greater than the net county cost.

NOW THEREFORE, BE IT RESOLVED, FOUND, DETERMINED, AND ORDERED, in regular session assembled on _____, that the Board of Supervisors authorizes ASSESSOR, to submit an application to participate in SCAPAP, in the form and manner specified by FINANCE, and hereby states that LACO agrees to provide the ASSESSOR with matching funds on a dollar-for-dollar basis in each fiscal year (2014-15, 2015-16, and 2016-17) that the ASSESSOR participates in the program, in accordance with Revenue and Taxation Code Section 95.5.

BE IT FURTHER RESOLVED, FOUND, DETERMINED, AND ORDERED that this resolution shall remain operative until rescinded, but in no event shall it remain operative beyond June 30, 2017, unless otherwise permitted or authorized by law.

Dated:_____ County of Los Angeles

By:_____

IT Security Policies – Department Feedback

August 21, 2014

Summary

- Proposed revisions to the 13 IT Security Policies were sent to all Department Heads and Chief Deputies on May 22, 2014.
- Six departments responded indicating support for the policies with no further changes (Auditor-Controller, Community and Senior Services, Fire, Health Services, Parks and Recreation, and Registrar-Recorder/County Clerk).
- Six departments provided feedback (Animal Care and Control, Executive Office, Internal Services, Public Health, Public Social Services, and Sheriff).
- No comments were provided for Policies 6.103 – Countywide Computer Security Threat Responses, 6.108 – Auditing and Compliance, and 6.112 – Secure Disposition of Computing Devices.
- Three overarching General Comments were submitted impacting several or all Policies resulting in a change to one.
- On the Policies, 32 comments were received. Changes were made on 16 and No Change recommended on remainder.

  Policy 6.100 – 3 comments received, change recommended to 1

  Policy 6.101 – 4 comments received, change recommended to 3

  Policy 6.101 Acceptable Use Agreement (AUA) – 7 comments received, change recommended to 6

  Policy 6.102 – 2 comments received, no changes being recommended

  Policy 6.104 – 3 comments received, change recommended to 2

  Policy 6.105 – 4 comments received, change recommended to 3

  Policy 6.106 – 1 comment received, no change being recommended

  Policy 6.107 – 1 comment received, no change being recommended

  Policy 6.109 – 3 comments received, no change being recommended

  Policy 6.110 – 4 comments received, change recommended to 1

Department Feedback	Department	Response
General Comments:		
1. Please remove the following paragraph from each 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".* If every Department was made aware of all security standards and procedures AND it was attached to the policy, then it might make sense to include this paragraph. However, because the CIO's office is creating these standards and procedures as time goes on and there does not appear to be a good mechanism for all Departments to receive these standards and procedures, the Board of Supervisor's policies should be limited to the policies. As such, throughout each of your policies 6.100 through 6.112, please remove any reference to standards and procedures.	Executive Office	**CHANGE recommended** The objective of this language is to empower the County's Information Security Officer and the ISSC to take immediate and appropriate action to develop and implement tactical, operational procedures or standards in response to an occurring or recent cyber-attack or breach. Each document contains this language as they are the foundational Policy that these tactical or operational measures are aligned to. A change will be made to the language from: "County IT security standards and procedures" to "County IT security operational and technical standards and procedures" in an effort to clarify intent. Additionally, to provide greater awareness at the executive departmental level, new IT security operational and technical standards and procedures will be shared with the CIO Council and CIO Leadership Committee and then sent to Department Heads, Chief Deputies, and Administrative Deputies.
2. The use of "approved by designated County Department management" in these policies is too broad – it covers routine confidential HR information that is sent all the time without specific authorization from Dept management or policy… For example, if I e-mail a PE to my secretary, or to HR, I'm in violation. If I use my VoIP phone to tell coworkers that it's a coworker's birthday, I'm in violation. This concern affects Policies # 6.101, 6.104, 6.105 and 6.110.	Internal Services Public Health	**NO CHANGE recommended by County Counsel/CIO** The term "approved by designated County Department management" is to provide flexibility for each department to define what the appropriate management level should be based on the department's own established procedures.

Department Feedback	Department	Response
3. Please remove references to "Board of Supervisors Policy NO. 9.015 – County Policy of Equity". I have asked Mary Wickham, Executive Director CEOP, to review this section and it does not make sense to include it. If County Counsel recommended it to be included, please have that Counsel talk to Mary. Remove references to CPOE in Policies # 6.101, 6.104, 6.105 and 6.111.	Executive Office Public Health	**NO CHANGE recommended by CIO/DA/DHR** Following a meeting with Ms. Mary Wickham and after her review of Policies # 6.101, 6.104, 6.105 and 6.111, she concurred to include the CPOE references in the policies. Ms. Wickham also suggested revisions to add CPOE to the examples of inappropriate behavior cited in the policies.
Policy 6.100 – Information Technology and Security Policy		
1. The statement "The head of each County Department, in consultation with the CISO, shall ensure the designation of a full-time permanent county department employee (DISO)…." I think the phrase "*in consultation with the CISO*" needs to be clarified. If you want the Department Head to notify the CISO of the Department's DISO, that needs to be stated. *If the Department Head must receive approval to hire the DISO, then this language should be removed*.	Executive Office	**CHANGE recommended** This language was revised to require department's IT management/ Chief Information Officer to "notify the CISO when a change to their DISO has occurred".
2. Portable devices strike digital cameras and audio/video devices – not generally considered to be IT devices.	Internal Services Public Health	**NO CHANGE recommended by CIO** Portable devices such as digital cameras and audio/video devices have storage devices which may store personally identifiable information (PII), protected health information (PHI), and must be protected to mitigate risk.
3. The last bullet under the DISO section calls for the DISO to report security incidents to the CISO. The LASD DISO plans to provide high-level reports to the CISO and any reports pertaining to a security event that affects both LASD and another County Department.	Sheriff	**NO CHANGE recommended by CIO** LASD, through its security incident reporting is in accordance with Board policy # 6.109 – Security Incident Reporting.

Department Feedback	Department	Response
Policy 6.101 – Use of County Information Technology Resources		
1. Under "General", the Paragraph that states "County IT resources shall be accessed and used for County business purposes that have been approved by designated County Department management unless expressly authorized by the Board of Supervisors' Policy No. 6.105 – Internet Usage. Reference to 6.104 – Electronic Communication should also be included, if 6.104 is revised to also have an exception to limited use of electronic communication. Also the "Privacy" section should also include reference to 6.104 – Electronic Communication.	Executive Office	**CHANGE recommended** Language in the "General" paragraph was revised to; "County IT resources shall be accessed and used in accordance with each Department's policies, standards, and procedures." This enables Department to establish their own acceptable controls, as described in the "General" paragraph of Policy 6.100.
2. Privacy section – see previous comments about "only" and management approval.	Internal Services Public Health	**CHANGE recommended** Language in the "Privacy" paragraph was revised to; "Information that is accessed using County IT resources shall be used in accordance with each Department's policies, standards, and procedures. Such information shall not be exposed and/or disclosed to unauthorized individuals."
3. Confidentiality section – "and/or other County IT resources" is overly broad.	Internal Services Public Health	**NO CHANGE recommended by CIO** Language is intentionally broad as all possible IT resources cannot be included.
4. Good place to include language allowing the incidental usage of IT resources for devices (personal computer and smartphones), IM, email, internet, etc.	Internal Services Public Health	**CHANGE recommended** Agreed - language revised to allow incidental usage similar to Policy 6.105.

Department Feedback	Department	Response
Policy 6.101 – Use of County Information Technology Resources / Acceptable Use Agreement (AUA)		
1. Under items #7 (Business Purposes) and #13 (Electronic Communications) add the exceptions to policy 6.104. Strike #7	Executive Office Internal Services Public Health	**CHANGE recommended** Business Purposes (7) language was changed to; "I shall use County IT resources in accordance with my Department's policies, standards, and procedures." Changes were made to Policy 6.104 – Electronic Communications to state; "Electronic communications systems/applications/services (e.g., electronic mail, instant messaging, etc.) are provided as a County IT resource for conducting County business in accordance with Departmental policies and procedures."
2. 1st paragraph strike "only" – big difference between shall be used for business purposes and shall only. Or add-in incidental use language. That incidental use should cover computer, cell phone, tablet, photographs, documentation, etc.	Internal Services Public Health	**CHANGE recommended** Paragraph with "only" was deleted and, for consistency was replaced with; "Furthermore, I shall use County IT resources in accordance with my Department's policies, standards, and procedures."
3. "Except as expressly authorized by Board of Supervisors Policy No. 6.105" is used numerous times. However, in item #7, the word "provided" is used in place of "authorized". The revised Board Policy 6.105 itself also uses the phrase "Except as expressly authorized". For consistency, we would recommend replacing "provided" with "authorized".	Public Social Services	**CHANGE recommended** Changes made in 1 and 2 address this comment.
4. Strike #8 Approved Devices – new home computer to access health care enrollment needs department authorization?	Internal Services Public Health	**CHANGE recommended** #8 Approved Devices has been removed from the AUA.
5. #9 basically requires specific authorization to say or share anything on e-mail or on the phone (VoIP). To see why, see definition of County IT Resources. Completely unworkable.	Public Health	**NO CHANGE recommended by CIO** Policy 6.101 and its AUA are revised to require department authorization for sending/disseminating/exposing personal and confidential information. Reference to COUNTY IT resources has been removed.
6. #12 Internet – see previous comments about "only" and management approval.	Internal Services	**CHANGE recommended** Language revised to "in accordance with each Department's policies, standards, and procedures".

Department Feedback	Department	Response
7. #14 – This is not the best way to address this problem. See Oracle forum example above. It may be feasible to include this limitation if it is written more narrowly.	Public Health	**CHANGE recommended** Language revised in 6.104 and 6.105 for consistency to state: "in accordance with each Department's policies, standards, and procedures".
Policy 6.102 – Countywide Anti-virus Security		
1. Problem here with limiting use of Internet (6.105) on an employee's personally owned devices (when not doing County work).	Public Health	**NO CHANGE recommended by CIO/DA/DHR/A-C** This policy refers to County IT Resources only. Use of employee owned devices ti access County IT Resources will be addressed in a separate BYOD policy.
2. Antivirus software is not available for many "personally owned computing devices," or where it is available, is not viable, e.g., IOS, VoIP phones, PDAs, digital cameras, storage media, printers, scanners, Google Glass. So this part needs a limitation "where technically feasible."	Public Health	**NO CHANGE recommended by CIO/DA/DHR/A-C** This policy refers to County IT Resources only. Use of employee owned devices ti access County IT Resources will be addressed in a separate BYOD policy.
Policy 6.104 – Electronic Communications		
1. Remove reference to the County Policy of Equity. *Also add some exceptions to the limited personal used, similar to policy 6.105.*	Executive Office	**CHANGE recommended** CPOE reference previously addressed and exception language for limited personal use is incorporated in this policy.
2. Globally change "systems/applications/services" to "services" and define the electronic communication services to include systems and applications.	Public Health Internal Services	**NO CHANGE recommended by CIO/DA/DHR/A-C** Change not required.
3. "Monitoring the access to, and use of County IT resources by County IT users must be approved in accordance…" Not clear what those applicable policies and laws are (need a reference?). Regarding the obligation to report to the A-C, it's any evidence of violation of "this policy." Is that intended to refer to the paragraph in which it appears or to the whole policy? Unclear, which will lead to problems in compliance and enforceability.	Public Health	**CHANGE recommended** Language revised to specifically state applicable policies; "Monitoring the access to, and use of County IT resources by County IT users must be approved in accordance with applicable policies (e.g., Board of Supervisors Policies Nos. 6.108 and 9.040, and County's Fiscal Manual) and laws on investigations. If any evidence of violation of this policy is identified, the Auditor-Controller's Office of County Investigations must be notified immediately."

Department Feedback	Department	Response
Policy 6.105 – Internet Usage Policy		
1. Under the statement "operating a private business or web site", *add the words* "non-county related" before website.	Executive Office	**CHANGE recommended** Example of inappropriate access language revised to "Operating a private business or a non-County business related web site".
2. Disagree with Internet storage site limitation. Some limits are necessary, but this is overly broad. For example, the State sets up a SharePoint, Box, or Dropbox site for a collaborative project that does not deal with sensitive or confidential data. Explicit written management approval is too cumbersome in this case. Internet file storage sites are now part and parcel of the way the world does business. The prohibition should be narrowed to affect only sensitive and confidential information on consumer sites.	Public Health	**CHANGE recommended** Revised language to add specificity relating to PII, PHI, and confidential / sensitive data when using Internet storage sites.
3. This policy also needs to address County-provided Internet file storage sites, such as OneDrive. Does this policy prohibit OneDrive use without specific management authorization?	Public Health	**CHANGE recommended** Language revised for departmental management to have discretion on usage of file storage sites such as OneDrive.
4. "Monitoring access…." This paragraph need not appear here. It's covered in 6.104, and more appropriately there.	Public Health	**NO CHANGE recommended by CIO/DA/DHR/A-C** These policies have to remain independent. Each policy has two distinct bodies of law.
Policy 6.106 – Physical Security		
1. Many County Departments are in older buildings where some of their IT areas may be unrestricted. For example, the policy includes telephone closets, which in the Hall of Administration, there are several Departments that will be out of compliance. *Either funding is provided for this policy, or this policy needs to be changed to address some of the physical limitations on securing all IT areas*, as defined in the policy.	Executive Office	**NO CHANGE recommended by CIO/DA/DHR/A-C** Departments should identify and determine these risks and work towards mitigating them. Funds, if necessary, should be requested during the budget process.
Policy 6.107 – IT Risk Assessment		
1. Not sure how this applies to contractors. Contractors can't violate the policy because the obligation is on the Department, not on the contractor.	Public Health	**NO CHANGE recommended by CIO/DA/DHR/A-C** This policy is associated with County IT Resources, not specific to contractors' resources. Risk assessments for contractors shall be addressed within its contract language (e.g., audit provision).

Department Feedback	Department	Response
Policy 6.109 – Security Incident Reporting		
1. The second paragraph calls for the DISO to report security incidents to the CISO. The LASD DISO plans to provide high-level reports to the CISO and any reports pertaining to a security event that affects both LASD and another County Department. Also, LASD conducts all criminal investigation relating to its employees. 2. The paragraph titled "Office of County Investigations (OCI)" will not be applicable to LASD. LASD conducts all violations of policy, security incidents, and criminal investigations internally, and there will be no reporting to the OCI. 3. The last paragraph does not seem to be consistent with California Civil Code Section 1798.29 where reporting is not required if the data was encrypted at rest.	Sheriff	**NO CHANGE recommended by CIO/DA/DHR/A-C** LASD reinstating their position consistent in their feedback for policy #6.100, which has not differ since adoption of the Board IT Security Policies in July 2004. Additionally, specific to California Civil Code Section 1798.29 where reporting is not required if the data was encrypted at rest is true from a state perspective. The CISO collects metric data to quantify security incidents that includes encrypted data and unencrypted data use for the measurement of the Countywide Information Security Program, not security breach reporting.
Policy 6.110 – Protection of Information on Portable Computing Devices		
1. The paragraph that states " 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 approval from designated County Department management……..." *is not feasible.* One way to perhaps address this is to make a general awareness statement in the AUA, *so employees know that there are risks posed with placing County data on a portable computing device not owned or operated by the County. The other possibility is looking into requiring encrypted devices, but that may also require funding for some, if not all Departments.*	Executive Office	**CHANGE recommended** Reference paragraph has been deleted. Bullet items replace it stating: • Departments must ensure an encryption solution is available where the stored County information (i.e., personal, confidential (e.g., social security number, medical records), or otherwise sensitive (e.g., legislative data)) is protected using encryption; • The County IT user shall comply with, and the portable computing device shall comply with, all applicable County IT resources, policies, standards, and procedures including, without limitation: Board of Supervisors Policy No. 6.101;

Department Feedback	Department	Response
2. Instead of making it seem that approval has to be sought every time a personal/sensitive/confidential information needs to be transferred to a portable computing device, and the device has to encrypt the information; rather, have the initial approval, to access the personal/sensitive/confidential information, carry the additional requirement of making any portable computing device carrying such information encrypt that information. This would then put the onus of securing the data on the person, who already has the approval/authority to access the information, to make provisions for the secure transport of such information.	Animal Care & Control	**NO CHANGE recommended by CIO/DA/DHR/A-C** Comment relating to downloading an approval form has been deleted from this policy. See 1 above.
3. "Protection of Information on Portable Computing Devices", on page 2, section A, in the third paragraph and first bullet of Section A, the language implies that personal and/or confidential information can be placed/stored on a portable device not owned or provided by the County, as long as it is approved by at least the DISO and the information is encrypted. Because Policy 6.100 includes smartphones within the definition of "portable devices", is the intent that a user will be able to store such personal and/or confidential information on a personal smartphone, once a BYOD policy is approved? If so, we recommend that this be reconsidered.	Public Social Services	**CHANGE recommended** Departments shall ensure that County data containing PII and PHI is encrypted.
4. The first bullet point under section A) does not seem to be a good fit for LASD. We don't require our users to obtain management approval before they store data on portable storage devices. We are in the process of installing removable media encryption on all LASD computers, and we already have a good percentage of our computers covered. This prevents the inappropriate disclosure of LASD data stored on such devices in case they are lost or stolen. We recommend this section to be removed.	Sheriff	**CHANGE recommended** Departments shall ensure that County data containing PII and PHI is encrypted.

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

To establish a countywide information technology (IT) security program supported by countywide policies within the Board of Supervisors Policy Manual (Manual) chapter 6 including related policies in other chapters of the Manual (e.g., chapters 3, 7, and 9) to assure appropriate and authorized access, usage, and integrity of County IT resources.

REFERENCE

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

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

California Civil Code Section 1798.29

POLICY

Definitions

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

- Computing devices, including, without limitation, the following:
    - Desktop personal computers, including, without limitation, desktop computers and thin client devices
    - Portable computing devices, including, without limitation, the following:
        - Portable computers, including, without limitation, laptops and tablet computers, and mobile computers that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to County IT resources; and
        - Portable devices, including, without limitation, personal digital assistants (PDAs), digital cameras, smartphones, cell phones, pagers, wearable computers (also known as body-borne computers or wearables), and audio/video recorders; and
        - Portable storage media, including, without limitation, diskettes, tapes, DVDs, CDs, USB flash drives, memory cards, and external hard disk drives; and
    - Multiple user and application computers, including, without limitation, servers
    - Printing and scanning devices, including, without limitation, printers, copiers, scanners, and fax machines
    - Network devices, including, without limitation, firewalls, routers, and switches.
- Telecommunications (e.g., wired and wireless), including, without limitation, voice and data networks, voicemail, voice over Internet Protocol (VoIP), and videoconferencing
- Software, including, without limitation, application software, operating systems software, and stored instructions
- Information, including, without limitation, the following:
    - Data
    - Documentation
    - Electronic communications (e.g., email, text message)
    - Personal information
    - Confidential information
    - Voice recordings
    - Photographs
    - Electronically stored information (data that is created, altered, communicated and stored in digital form)
- Services, including, without limitation, hosted services and County Internet services
- Systems, which are an integration and/or interrelation of various components of County IT resources to provide a business solution (e.g., eCAPS).

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

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

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

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

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

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

General

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

- Privacy and confidentiality
- Information integrity, including, without limitation, data integrity
- Availability
- Accountability
- Appropriate access, use, exposure, disclosure, and modification

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

RESPONSIBILITIES

County Departments

The head of each County Department is responsible for ensuring County IT security, including, without limitation, within the County Department. Management of each County Department is responsible for organizational adherence to countywide County IT resources policies, standards, and procedures and countywide County IT security policies, operational and technical 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.

Chief Information Officer (CIO)

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

Chief Information Security Officer (CISO)

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

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

County Department IT Management / Departmental Chief Information Officer

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

- Manage County IT resources within the County Department
- Shall notify the CISO when a change to their DISO has occurred

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

Departmental Information Security Officer (DISO)

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

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

County IT Users

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

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

Information Security Steering Committee (ISSC)

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

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

- Assisting the CISO in developing, reviewing, and recommending countywide County IT security policies
- Identifying and recommending industry best practices for countywide County IT security
- Developing, reviewing, recommending, and approving countywide County IT security technical and operational standards, procedures, and guidelines
- Coordinating communication and collaboration among County Departments on countywide and County Department IT security issues
- Coordinating countywide County IT security education and awareness

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

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

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

To establish policies for use of County information technology (IT) resources.

REFERENCE

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

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

Board of Supervisors Policy No. 6.104 – Electronic Communications

Board of Supervisors Policy No. 6.105 – Internet Usage Policy

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

California Civil Code Section 1798.29

POLICY

General

This policy is applicable to all County IT users.

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

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

County IT users cannot expect any right to privacy concerning their activities related to County IT resources, including, without limitation, in anything they create, store, send, or receive using County IT resources. Having no expectation to any right to privacy includes, for example, that County IT users' access and use of County IT resources may be monitored or investigated by authorized persons at any time, without notice or consent.

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

County IT resources shall be accessed and used in accordance with each Department's policies, standards, and procedures.

County IT resources may not be used:

- For any unlawful purpose;
- For any purpose detrimental to the County or its interests;
- For personal financial gain;
- In any way that undermines or interferes with access to or use of County IT resources for official County purposes;
- In any way that hinders productivity, efficiency, customer service, or interferes with a County IT user's performance of his/her official job duties;
- To express or imply sponsorship or endorsement by the County, except as approved in accordance with Department's policies, standards, and procedures, or;
- For personal purpose where activities are for private gain or advantage, or an outside endeavor not related to County business purpose, personal purpose does not include the incidental and minimal use of County IT resources, such as internet usage, for personal purposes, including an occasional use of the internet.

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

The County has the right to administer any and all aspects of County IT resources access and other use, including, without limitation, the right to monitor Internet, electronic communications (e.g., email, text messages, etc.), and data access. Access to County IT resources is a privilege, which access may be modified or revoked at any time, without notice or consent.

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

Access Control

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

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

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

Authentication

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

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

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

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

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

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

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

Information Integrity

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

Accessing County IT Resources Remotely

Remote access to County IT resources by a County IT user shall require approval by designated County Department management. Each County IT user shall comply with, and only use equipment (e.g., County-owned computing device and personally owned computing device) that complies with, all applicable County IT resources policies, standards, and procedures, including, without limitation:

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

Without limiting the foregoing, County IT users who are authorized to remotely access County IT resources using personally owned computing devices shall ensure that antivirus software which is installed and up-to-date, operating system software and application software which are up-to-date (e.g., critical updates, security updates, and service packs), and firewall (i.e., software firewall on the computing device or hardware firewall) which is installed and up-to-date.

Privacy

Information that is accessed using County IT resources shall be used in accordance with each Department's policies, standards, and procedures. Such information shall not be exposed and/or disclosed to unauthorized individuals.

Confidentiality

Unless specifically authorized by designated County Department management, sending, disseminating, or otherwise exposing and/or disclosing personal and/or confidential information is strictly prohibited. This includes, without limitation, information that is subject to HIPAA, the HITECH Act, or any other confidentiality or privacy legislation.

Definition Reference

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

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

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

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

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

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

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to

termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

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

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

ANNUAL

As a County of Los Angeles (County) employee, contractor, subcontractor, volunteer, or other authorized user of County information technology (IT) resources, I understand that I occupy a position of trust. Furthermore, I shall use County IT resources in accordance with my Department's policies, standards, and procedures. I understand that County IT resources shall not be used for:

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

I shall maintain the confidentiality of County IT resources (e.g., business information, personal information, and confidential information).

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

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

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

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

2. No Expectation of Privacy: I do not expect any right to privacy concerning my activities related to County IT resources, including, without limitation, in anything I create, store, send, or receive using County IT resources. I understand that having no expectation to

any right to privacy includes, for example, that my access and use of County IT resources may be monitored or investigated by authorized persons at any time, without notice or consent.

3. Activities related to County IT resources: I understand that my activities related to County IT resources (e.g., email, instant messaging, blogs, electronic files, County Internet services, and County systems) may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall not either intentionally, or through negligence, damage, interfere with the operation of County IT resources. I shall neither, prevent authorized access, nor enable unauthorized access to County IT resources responsibly, professionally, ethically, and lawfully.

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

5. Security access controls: I shall not subvert or bypass any security measure or system which has been implemented to control or restrict access to County IT resources and any related restricted work areas and facilities. I shall not share my computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, SecurID cards/tokens, biometric logons, and smartcards).

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

7. Business purposes: I shall use County IT resources in accordance with my Department's policies, standards, and procedures.

8. Confidentiality: I shall not send, disseminate, or otherwise expose or disclose to any person or organization, any personal and/or confidential information, unless specifically authorized to do so by County management. This includes, without limitation information that is subject to Health Insurance Portability and Accountability Act of 1996, Health Information Technology for Economic and Clinical Health Act of 2009, or any other confidentiality or privacy legislation.

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

10. Offensive materials: I shall not access, create, or distribute (e.g., via email) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County IT resources (e.g., over County-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless authorized to do so as a part of my assigned job duties (e.g., law enforcement). I shall report to my management any offensive materials observed or received by me on County IT resources.

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 in accordance with my Department's policies and procedures. I understand that my use of the County Internet services may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time. I shall comply with all County Internet use policies, standards, and procedures. I understand that County Internet services may be filtered, but in my use of them, I may be exposed to offensive materials. I agree to hold County harmless from and against any and all liability and expense should I be inadvertently exposed to such offensive materials.

12. Electronic Communications: I understand that County electronic communications (e.g., email, text messages, etc.) created, sent, and/or stored using County electronic communications systems/applications/services are the property of the County. All such electronic communications may be logged/stored, may be a public record, and are subject to audit and review, including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time, without notice or consent. I shall comply with all County electronic communications use policies, standards, and procedures and use proper business etiquette when communicating over County electronic communications systems/applications/services.

13. Public forums: I shall only 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) in accordance with Department's policies, standards, and procedures.

14. Internet storage sites: I shall not store County information (i.e., personal, confidential (e.g., social security number, medical record), or otherwise sensitive (e.g., legislative data)) on any Internet storage site in accordance with Department's policies, standards, and procedures.

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

16. Compliance with County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements: I shall comply with all applicable County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements relating to County IT resources. These include, without limitation, Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy, Board of Supervisors Policy No.

6.101 – Use of County Information Technology Resources, and Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

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

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

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

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

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

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

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

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

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

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

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

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

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

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

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

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

To establish an antivirus (e.g., anti-spyware, anti-spam) security policy for the protection of all County information technology (IT) resources.

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

POLICY

This policy is applicable to all County IT users.

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

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

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

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

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

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

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

Remote access to County IT resources by a County IT user shall require approval by designated County Department management. The County IT user shall comply with, and only use equipment (e.g., County-owned computing device and personally owned computing device) that complies with, all applicable County IT resources policies, standards, and procedures, including, without limitation:

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

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

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

The purpose of this policy is to define the County's responsibility in responding to security threats affecting the confidentiality, integrity, and/or availability of County information technology (IT) resources.

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

POLICY

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

The County shall establish a Countywide Computer Emergency Response Team (CCERT). The CCERT shall be led by the Chief Information Security Officer (CISO) and shall consist of representatives from all County Departments. CCERT shall communicate security information, guidelines for notification processes, identify potential security risks, and coordinate responses to thwart, mitigate, or eliminate

security threats to County IT resources.

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

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

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

Each County Department shall establish and implement Departmental Computer Emergency Response Procedures. The DCERT shall inform the CCERT, as early as possible, of security threats to County IT resources.

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

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

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

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

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

Definition Reference

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.104	**Electronic Communications**	**07/13/04**

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.105 – Internet Usage Policy

Board of Supervisors Policy No. 6.108 – Auditing and Compliance

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

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

within County Government

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

California Civil Code Section 1798.29

POLICY

This policy is applicable to all County IT users.

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

County electronic communications are provided as a County IT resource for conducting County business purposes. Any other use must be minimal or incidental as set forth in Board of Supervisors Policy No. 6.105 – Internet Usage Policy and may not be a use which is substantial enough to result in a gain or advantage to the user or a loss to the County for which a monetary value may be estimated.

Electronic communications systems/applications/services (e.g., electronic mail, instant messaging, etc.) are provided as a County IT resource for conducting County business in accordance with Departmental policies and procedures.

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

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

All electronic communications created, sent, and/or stored using County electronic communications systems/applications/services are the property of the County. All such electronic communications may be logged/stored, may be a public record, and are subject to audit, review, and discovery including, without limitation, periodic monitoring and/or investigation, by authorized persons at any time as directed by designated

County Department management.

Monitoring the access to, and use of County IT resources by County IT users must be approved in accordance with applicable policies (e.g., Board of Supervisors Policies Nos. 6.108 and 9.040, and County's Fiscal Manual) and laws on investigations. If any evidence of violation of this policy is identified, the Auditor-Controller's Office of County Investigations must be notified immediately.

The following are examples of inappropriate access or use of County IT resources, including without limitation County electronic communication services. This is not a comprehensive list of all possible violations:

- Downloading, accessing, storing, displaying or distributing software, unless approved by designated County Department management
- Downloading, accessing, storing, displaying, viewing or distributing material (e.g., movies, music, software, and books) in violation of copyright laws
- Downloading, accessing, storing, displaying, viewing or distributing pornography or other sexually explicit material
- Soliciting participation in, or advertising scams (e.g., spamming, pyramid schemes, and "make-money-fast" schemes) to others
- Posting or transmitting libelous, defamatory, fraudulent, or confidential information
- Operating a private business or a non-County business related web site
- Posting or transmitting to unauthorized persons any material deemed to be confidential, personal, or otherwise protected from disclosure
- Participating in partisan political activities
- Attempting unauthorized access to the account of another person or group on the Internet, or attempting to circumvent County security measures, or security measures taken by others connected to the Internet, regardless of whether or not such attempts are successful or result in corruption or loss of data or other information (e.g., password stealing, phishing, or whaling.
- Knowingly or carelessly distributing malicious code to or from County IT resources
- Accessing, creating, or distributing (e.g., via email) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County IT resources (e.g., over County-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless authorized to do so as a part of such County IT user's assigned job function (e.g., law enforcement).

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

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

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

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

Encryption use for email communications (e.g., create, send, store) using County electronic communications systems/applications/services may be appropriate when communicating externally to the County's network, or required in some instances, to secure the contents of electronic communications.

Definition Reference

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

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

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

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

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

Compliance

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-

County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

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

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.104 – Electronic Communications

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

California Civil Code Section 1798.29

POLICY

This policy is applicable to all County IT users.

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

County Internet services are provided as a County IT resource for conducting County business purposes. Any other use must be minimal or incidental and may not be a use which is substantial enough to result in a gain or advantage to the user or a loss to the County for which a monetary value may be estimated.

County IT resources, including without limitation County Internet services, may not be used:

- For any unlawful purpose;
- For any purpose detrimental to the County or its interests;
- For personal financial gain;
- In any way that undermines or interferes with access to or use of County IT resources for official County purposes;
- In any way that hinders productivity, efficiency, customer service, or interferes with a County IT user's performance of his/her official job duties;
- To express or imply sponsorship or endorsement by the County, except as approved in accordance with Department's policies and procedures; or
- For personal purpose where activities are for private benefit or advantage, or an outside endeavor not related to County business purpose. Personal purpose does not include the incidental and minimal use of County IT resources, such as occasional internet usage for personal purposes.

Unless specifically authorized by County management, sending, disseminating, or otherwise exposing and/or disclosing any non-public County information (e.g., software program code; business data, documentation or other information; personal data, documentation or related information; any confidential, legislative, or sensitive data, documentation, and other information) is prohibited in accordance with Board of Supervisors Policy No. 3.040 (see Reference section). This includes, without limitation, information protected from disclosure under HIPAA, the HITECH Act, or any applicable information confidentiality or privacy policy or legislation.

Except as expressly authorized below in this Board of Supervisors Policy No. 6.105, no County IT user shall access or use County IT resources to create, exchange, publish, or distribute in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) not specifically approved by designated County Department management.

County Departments may adopt and implement departmental policies and procedures for authorizing one or more specified individuals, as a part of each such individual's assigned job function, to use County IT resources to create, exchange, publish, or distribute in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, and other social networking services) information on behalf of the County Department that is not specifically approved by designated County Department management. Such departmental policies and procedures shall, at a minimum:

a) Require all information created, exchanged, published, or distributed otherwise to be in compliance with all applicable aspects of countywide County IT resources policies, standards, and procedures and countywide County IT security policies, standards, and procedures, as well as any additional policies, standards, and procedures established by the County Department;

b) Require the County Department to designate management to regularly monitor the information created, exchanged, published, or distributed in public forums by the specified individual(s); and

c) Require the County Department as quickly as practicable to address instances in which the specified individual(s) do not comply with the departmental policies and procedures.

No County IT user shall store County information (i.e., personal, confidential (e.g., social security number, medical record), or otherwise sensitive (e.g., legislative data)) on any Internet storage site without prior written approval by designated County Department management.

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.

County IT users must obtain designated County Department management approval to use County Internet services. Authorized users must not share their credentials, usernames, passwords, or allow another person to access County Internet services using their account.

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

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

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

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

The following are examples of inappropriate access or use of County IT resources, including without limitation County Internet services. This is not a comprehensive list of all possible violations:

- Downloading, accessing, storing, displaying or distributing software, unless approved by designated County Department management
- Downloading, accessing, storing, displaying, viewing or distributing material (e.g., movies, music, software, and books) in violation of copyright laws
- Downloading, accessing, storing, displaying, viewing or distributing pornography or other sexually explicit material
- Soliciting participation in, or advertising scams (e.g., spamming, pyramid schemes, and "make-money-fast" schemes) to others
- Posting or transmitting libelous, defamatory, fraudulent, or confidential information
- Operating a private business or a non-County business related web site
- Posting or transmitting to unauthorized persons any material deemed to be confidential, personal, or otherwise protected from disclosure
- Participating in partisan political activities
- Attempting unauthorized access to the account of another person or group on the Internet, or attempting to circumvent County security measures, or security measures taken by others connected to the Internet, regardless of whether or not such attempts are successful or result in corruption or loss of data or other information (e.g., password stealing, phishing, or whaling.
- Knowingly or carelessly distributing malicious code to or from County IT resources
- Accessing, creating, or distributing (e.g., via email) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County IT resources (e.g., over County-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless authorized to do so as a part of such County IT user's assigned job function (e.g., law enforcement).

Definition Reference

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

POLICY

This policy is applicable to all County IT users.

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

Facility Security Plan

Each County Department is required to have a Facility Security Plan, which shall include, without limitation, measures to safeguard County IT resources. The plan shall

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

Proper Identification

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

Access to Restricted IT Areas

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

Physical Security Controls

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

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

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

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

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

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

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

To ensure the performance of periodic information technology (IT) risk assessments of County Departments for the purpose of identifying security threats to, and security vulnerabilities within, County IT resources and initiating appropriate remediation.

REFERENCE

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

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

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

POLICY

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

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

IT risk assessments are mandatory and encompass information gathering, analysis,

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

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

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

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

Definition Reference

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

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

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

Compliance

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

Policy Exceptions

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

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

POLICY

This policy is applicable to all County IT users.

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

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

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

Definition Reference

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

California Civil Code Section 1798.29

POLICY

This policy is applicable to all County IT users.

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

All County IT security incidents shall be reported by the Departmental Information Security Officer (DISO) to the Chief Information Security Officer (CISO), as required by County IT security policies, standards, and procedures, upon discovery to minimize the risk to the County, its employees and assets, and other persons/entities, and to ensure compliance with applicable laws, and to facilitate the prosecution of criminal acts against County IT resources.

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

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

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

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

Chief Information Security Officer (CISO)

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

- Virus or worm outbreaks that infect computing devices, or appear to be crafted to targeted an individual user(s), department(s), resource or data;

- Malicious attacks on telecommunications;
- Web page defacements;
- Actual or suspected loss or use, exposure, disclosure, and modification of personal information and/or confidential information;
- Lost or stolen computing devices containing personal information and/or confidential information;
- Denial of Service or Distributed Denial of Service attacks;
- Malicious use of web-based applications;
- Unauthorized privilege escalation use of administrator credentials.

Chief HIPAA Privacy Officer

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

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

Office of County Investigations (OCI)

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

- System breaches from internal or external sources access and;
- Inappropriate non-work related information which may include, without limitation, music and videos to an extent that is not permitted by Board of Supervisors Policy No. 6.105 and pornography;
- Actual or suspected loss or use, exposure, disclosure, and modification of personal information and/or confidential information;
- Lost or stolen computing devices containing personal information and/or confidential information.

Chief Information Officer (CIO)

All County IT security incidents that affect multiple County Departments create significant loss of productivity, or result in the actual or suspected loss or disclosure of

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

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

Definition Reference

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

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

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

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

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

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

and Security Policy.

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

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

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

Compliance

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

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007 **Sunset Review Date: May 8, 2011**
Reissue Date: **Sunset Review Date:**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

California Civil Code Section 1798.29

POLICY

This policy is applicable to all County IT users.

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

A) Portable Computing Devices and Information

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

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

- Departments must ensure an encryption solution is available where the stored County information (i.e., personal, confidential (e.g., social security number, medical records), or otherwise sensitive (e.g., legislative data)) is protected using encryption;

- The County IT user shall comply with, and the portable computing device shall comply with, all applicable County IT resources, policies, standards, and procedures including, without limitation: Board of Supervisors Policy No. 6.101;

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

- Board of Supervisors Policy No. 6.106 – Physical Security;

- Board of Supervisors Policy No. 6.109 – Security Incident Reporting;

- Inclusion of this Board of Supervisors Policy No. 6.110 – Protection of Information on Portable Computing Devices; and

- Board Policy No. 6.112 – Secure Disposition of Computing Devices.

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 is 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 a portable computing device is lost or stolen and the stored data is not encrypted, the County Department shall be able to recreate the personal information and/or confidential information with 100 percent accuracy and shall be able to provide notification to the affected persons/entities in accordance with Board of Supervisors Policy .

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 shall be taken to minimize the amount of information stored on the device. Additionally, if feasible, such information shall be abbreviated or redacted to limit exposure (e.g., last 4 digits of a Social Security number).

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

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

Definition Reference

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

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

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

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

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

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

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

Compliance

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

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007
Reissue Date:

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

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

To ensure that the appropriate level of information security awareness training is provided to all County information technology (IT) users.

REFERENCE

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

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

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

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

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

POLICY

This policy is applicable to all County IT users.

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

County Departments shall work with the Chief Information Office to establish and maintain a departmental information security awareness training program.

Information security programs at County Departments shall include, without limitation, information security awareness training that is based on the County Department's information technology use and security policies and which includes, without limitation, training in the handling and protection of personal information and/or confidential information and in a County IT user's responsibility to notify County Department management in the event of actual or suspected loss or disclosure of personal information and/or confidential information.

For County employees, training shall begin with County employee orientation and shall be conducted on a periodic basis throughout a County employee's term of employment with the County.

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

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

Information security awareness training shall be provided to County IT users as appropriate to their job function, duties, and responsibilities.

Definition Reference

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

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

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

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

As used in this policy, the terms "personal information" and "confidential information"

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007 **Sunset Review Date: May 8, 2011**

Reissue Date: **Sunset Review Date:**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

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

POLICY

This policy is applicable to all County IT users.

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

Each County Department is responsible for ensuring that all information and software

on County-owned or leased computing devices are rendered unreadable and unrecoverable, whether or not removed from such computing devices, prior to disposition of such computing devices out of County inventory, to prevent unauthorized use or disclosure.

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

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

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

• Computing device sent to salvage

• Computing device destroyed

• Computing device donated to a non-County organization

Definition Reference

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

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

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

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

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

Security Policy.

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

Compliance

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

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: October 23, 2007 **Sunset Review Date: October 23, 2011**
Reissue Date: **Sunset Review Date:**