



WILLIAM T FUJIOKA
Chief Executive Officer

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

DATE: April 3, 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) **Legacy System Replacement Status Presentation**
Assessor – Steven Hernandez or designee
 - B) **Proposed Revisions to IT Security Policies 6.100 – 6.112**
CIO – Richard Sanchez or designee
2. Public Comment
3. Adjournment

LEGACY REPLACEMENT STATUS



Scott Thornberry, Program Manager
Dan Gielan, Enterprise Architect
March 27, 2014

1



The Challenge

- Aging Technology Environment
 - 120+ stovepipe applications
 - Applications are difficult to maintain and risky to enhance
 - Functionality is limited and does not support Dept. needs
 - Complex , high-volume, and paper-intensive environment
- At Risk:
 - \$14 billion in property tax revenue to the State, County, and School Districts

2



The Response

- Hired outside consultant to assist in this undertaking
- Established modernization roadmap with 3 major initiatives:
 1. Replacement of Legacy Systems
 2. Data Quality Management
 3. Document Management



3



Due Diligence

1. Explored and evaluated all available commercial assessment software products (COTS)
2. Explored and evaluated what other California Counties have done / are doing



Page 4



COTS Products

The Assessor evaluated 7 major products designed or in some stage of design for California assessment



5



Other Counties' Approaches

- **Self Development (Build):**
 - Replatforming
 - Build from scratch (leveraging existing)
- **Buy and build:**
 - Buy (mostly as-is)
 - Buy partial and interface (band-aid approach)
 - Buy base product and build California functionality



6

Product Evaluation Results

	A	B	C	D	E *	F	G
How close is it to our ideal?							
May we modify the product?							
Is it maintainable?							
Can it be easily changed?							
Can resources be obtained?							
Will the vendor be a good partner?							
Can it be done in reasonable time?							
Overall rating							

Highest Rating
 Mid-High Rating
 Mid-Low Rating
 Lowest Rating



Findings

No existing product meets our needs



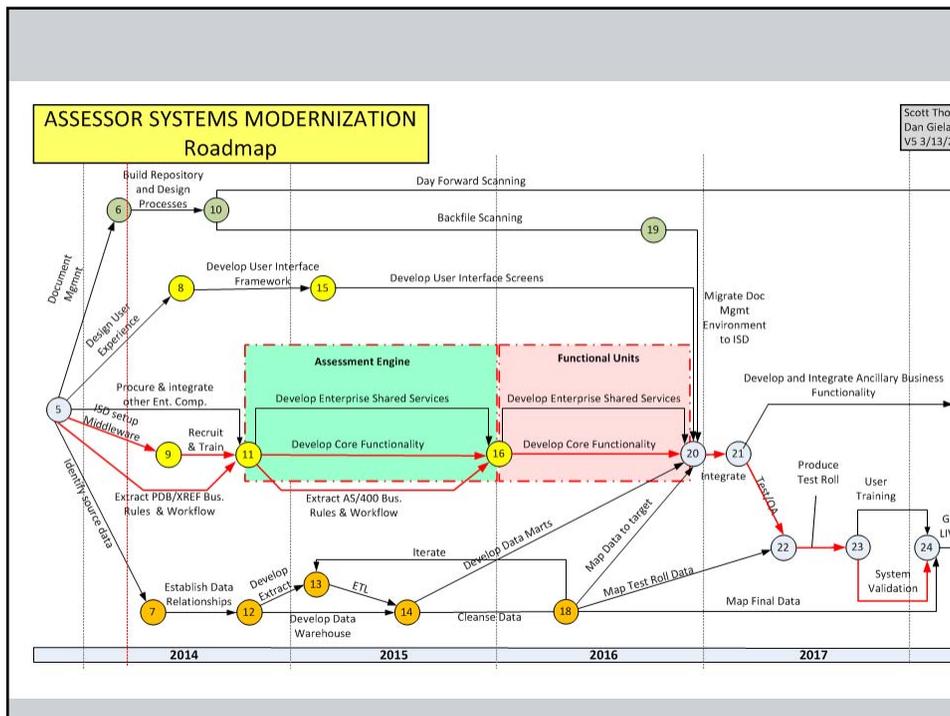
8

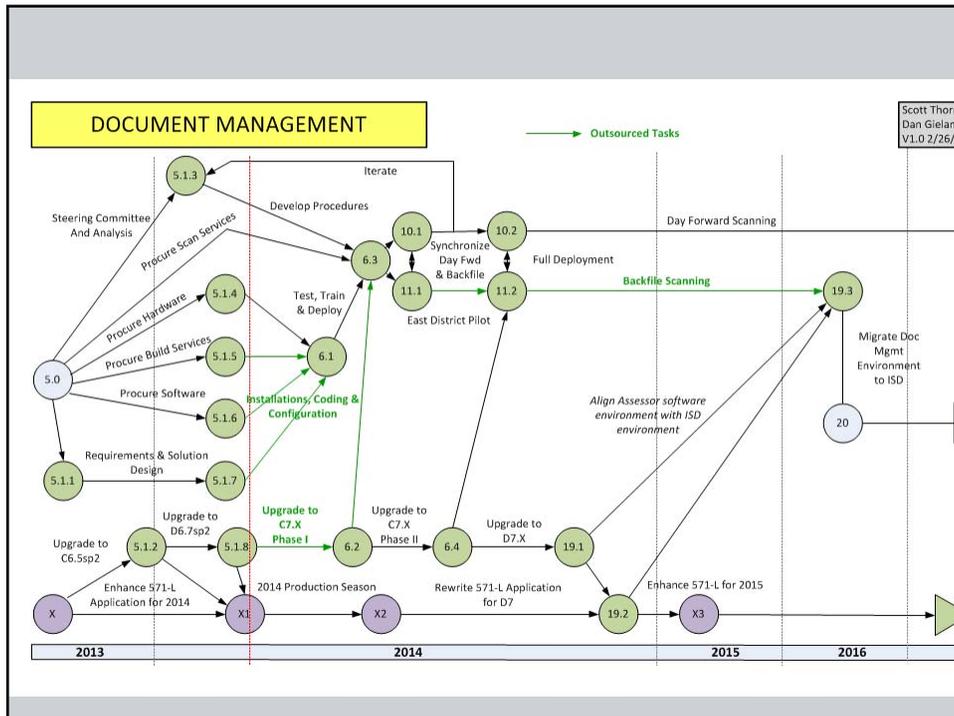
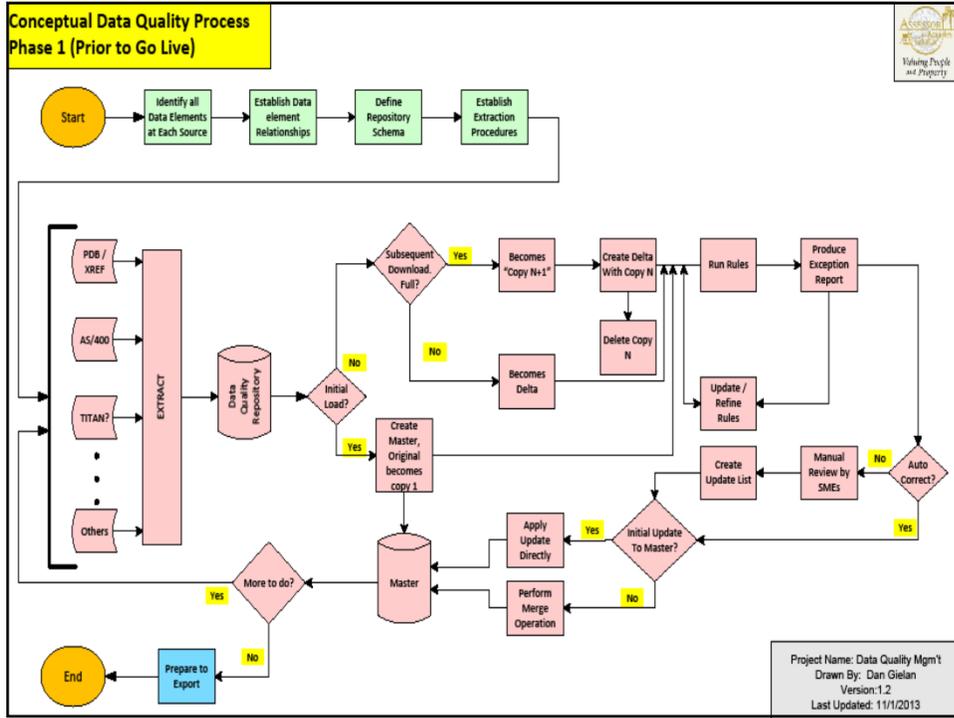


Solution

Create a tailor made
enterprise system
(leverage, buy, build, integrate).

9







Implementation

- Create the enterprise framework based on COTS components (leveraging LACO infrastructure where possible)
 - Rules Engine (BRE), Workflow (BPM), SOA, ESB, ECM, etc.
- Create the functional framework
 - Valuation and Assessment tools
- Develop and Integrate (leveraging existing systems)

13



Timeline

Activity	Timeframe
Evaluation and Decisions	7/1/2013 - 3/1/2014
Obtain Enterprise Components	11/1/2013 - 7/1/2014
Ramp up initial design and framework	7/1/2014 – 9/30/2014
Agile development to close gaps	10/1/2014 – 7/1/2017
Parallel execution of 2017 roll	7/15/2017
Compare executions results and identify each and every deviation	7/15/2017 – 1/2/2018
Initial go live	1/2/2018

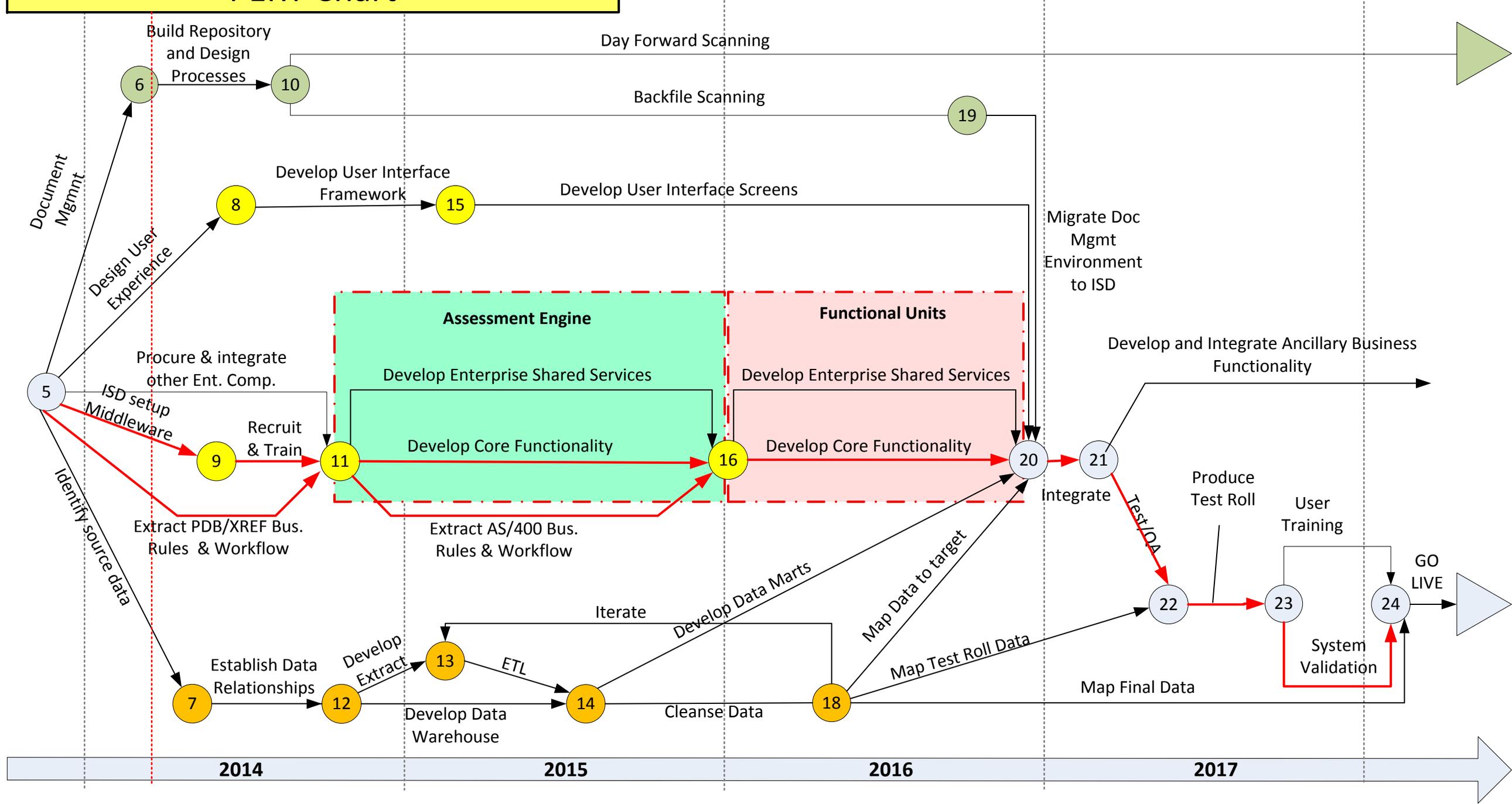
14

Questions and Answers

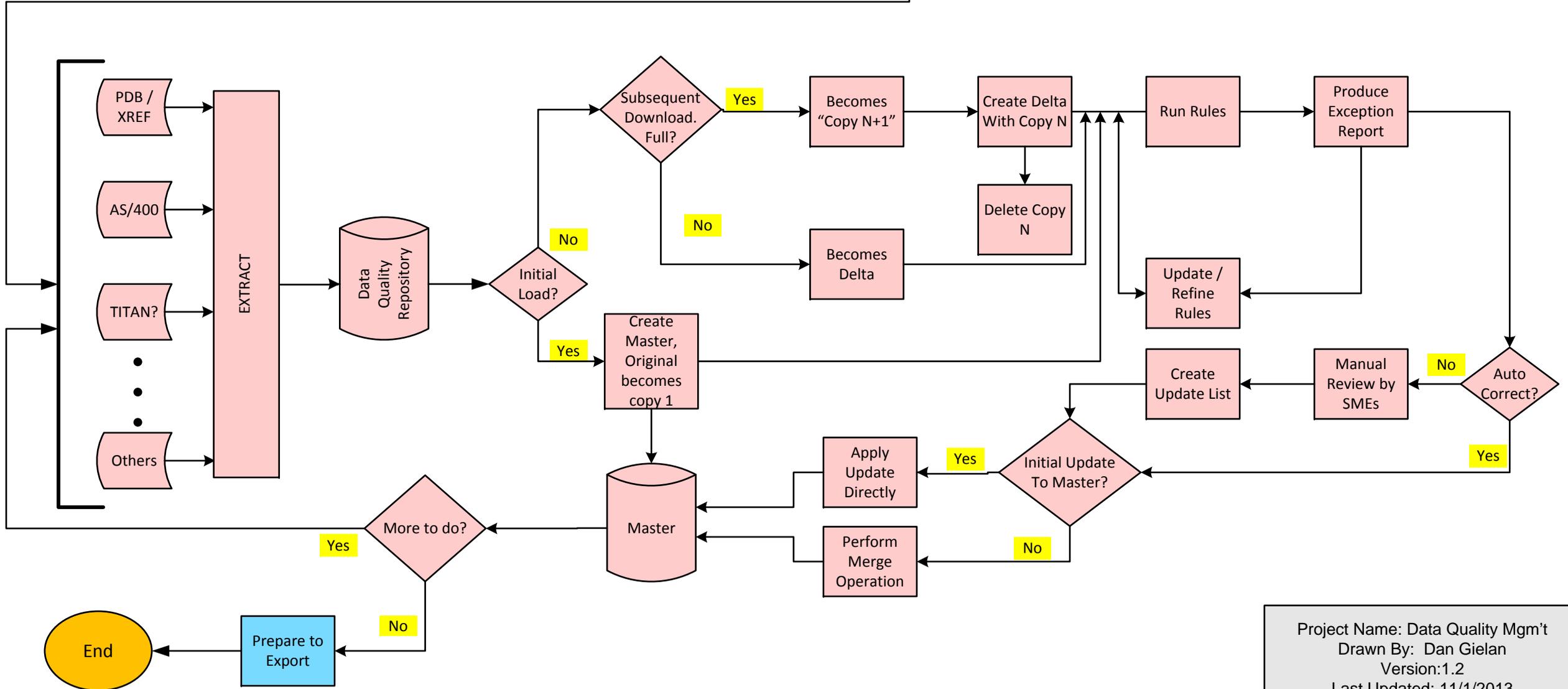
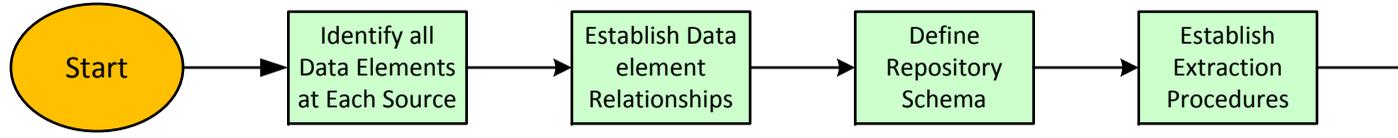


ASSESSOR SYSTEMS MODERNIZATION PERT Chart

Scott Thornberry
Dan Gielan
V5 3/13/2014

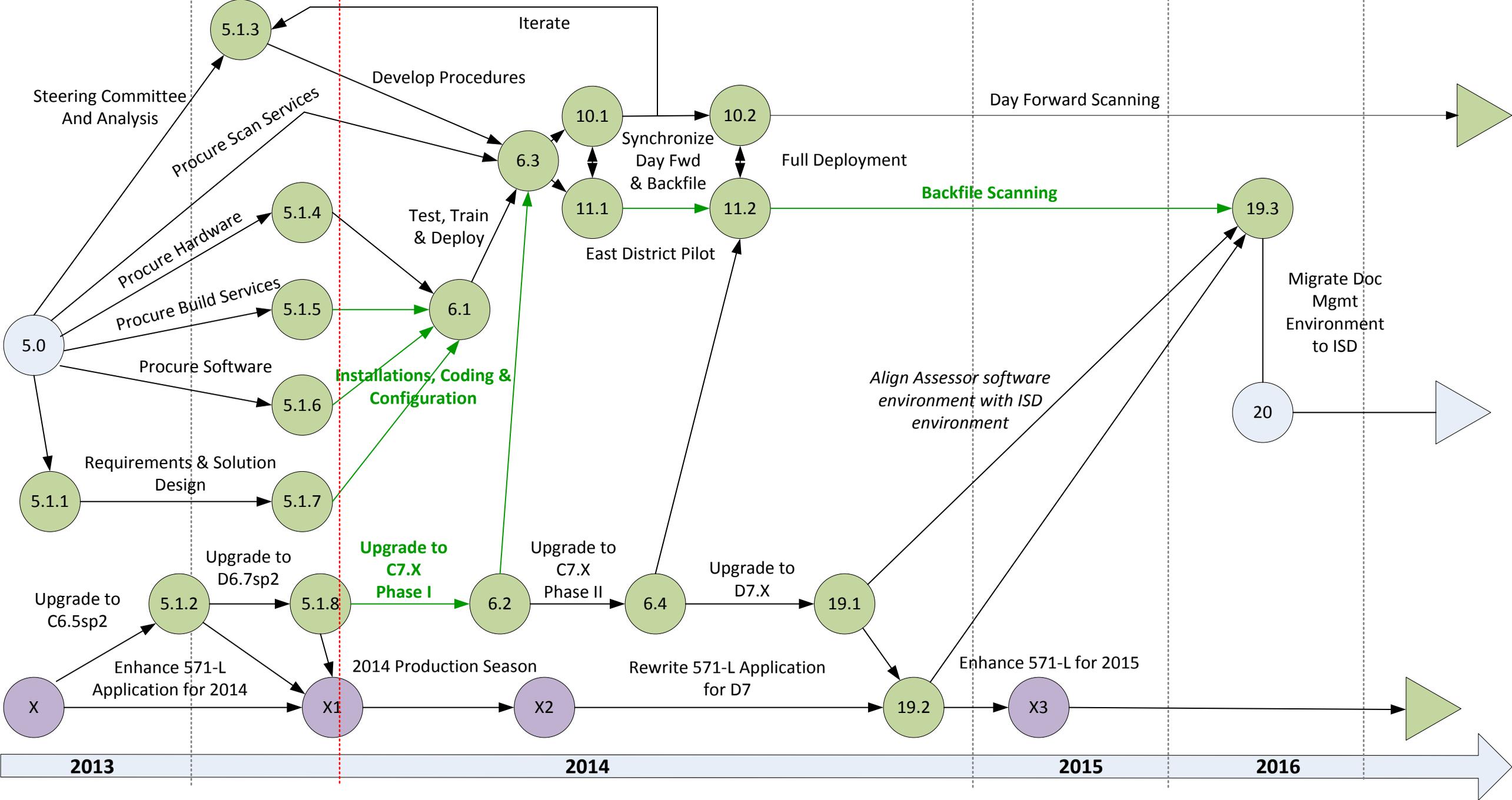


Conceptual Data Quality Process Phase 1 (Prior to Go Live)



DOCUMENT MANAGEMENT

Scott Thornberry
Dan Gielan
V1.0 2/26/2014



Summary of Proposed Revisions to IT Security Policies 6.100 – 6.112

Policy 6.100 – Information Technology and Security Policy

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

Policy 6.101 – Use of County Information Technology Resources

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

Policy 6.102 – Countywide Antivirus Security Policy

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

Policy 6.103 – Countywide Computer Security Threat Responses

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

Policy 6.104 – Electronic Communications

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

Policy 6.105 – Internet Usage Policy

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

Policy 6.106 – Physical Security

- ✓ No changes other than extending sunset review date.

Policy 6.107 – Information Technology Risk Assessment

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

Policy 6.108 – Auditing and Compliance

- ✓ No changes other than extending sunset review date.

Policy 6.109 – Security Incident Reporting

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

Policy 6.110 – Protection of Information on Portable Computing Devices

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

Policy 6.111 – Information Security Awareness Training

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

Policy 6.112 – Secure Disposition of Computing Devices

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



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

[California Civil Code Section 1798.29](#)

POLICY

Definitions

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

- Computing devices, including, without limitation, the following:
 - Desktop personal computers, including, without limitation, desktop computers and thin client devices
 - Portable computing devices, including, without limitation, the following:
 - Portable computers, including, without limitation, laptops and tablet computers, and
 - Mobile computers are portable computing devices that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to the County’s IT resources; and
 - Mobile computers that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to County IT resources; and infrastructure and/or application system(s)
 - Portable devices, including, without limitation, personal digital assistants (PDAs), digital cameras, smartphones, cell phones, and pagers, wearable computers (also known as body-borne computers or wearables), and audio/video recorders; and
 - Portable storage media, including, without limitation, diskettes, tapes, DVDs, CDs, USB flash drives, memory cards, and external hard disk drives; and
 - Multiple user and application computers, including, without limitation, servers
 - Printing and scanning devices, including, without limitation, printers, copiers, scanners, and fax machines
 - Network devices, including, without limitation, firewalls, routers, and switches.
- Telecommunications (e.g., wired and wireless), including, without limitation, voice and data networks, voicemail, voice over Internet Protocol (VoIP), and videoconferencing
- Software, including, without limitation, application software ~~and~~, operating systems software, and stored instructions
- Information, including, without limitation, the following:
 - Data
 - Documentation
 - Electronic communications mail (e.g., email, text message)
 - Personal information
 - Confidential information
 - Voice recordings

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

- Services, including, without limitation, hosted services and County Internet services
- Systems, which are an integration and/or interrelation of various components of County IT resources to provide a business solution (e.g., eCAPS).

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

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

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

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

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

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

General

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

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

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

RESPONSIBILITIES

County Departments

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

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

Chief Information Officer (CIO)

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

Chief Information Security Officer (CISO)

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

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

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

County Department IT Management / Departmental Chief Information Officer

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

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

Departmental Information Security Officer (DISO)

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

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

County IT Users

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

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

Countywide Computer Emergency Response Team (CCERT)

[Include Definition?]

Departmental Computer Emergency Response Team (DCERT)

[Include definition?]

Information Security Steering Committee (ISSC)

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

[California Civil Code Section 1798.29](#)

POLICY

General

This policy is applicable to all County IT users.

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

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

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

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

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

County IT resources shall be accessed and used only for County County management approved business purposes that have been approved by designated County Department management only; unlessexcept expressly authorized by Board of Supervisors' Policy No. 6.105 – Internet Usage.

County IT resources, may not be used:

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

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

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

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

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

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

Access Control

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

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

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

Authentication

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

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

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

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

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

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

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

Information Integrity

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

Accessing County IT Resources Remotely

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

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

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

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

~~, antivirus software which is installed and up-to-date, operating system software and application software which are up-to-date (e.g., critical updates, security updates, and service packs), and firewall (i.e., software firewall on the computing device or hardware firewall) which is installed and up-to-date.~~

Privacy

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

Confidentiality

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

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:

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

ANNUAL**

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

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

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

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

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

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

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

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

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

5.7. ~~Approved b~~Business purposes: Except as expressly provided by Board of Supervisors Policy No. 6.105 – Internet Usage, I shall use County IT resources only for ~~County management approved~~ business purposes approved by designated County ~~d~~Department management only. I understand that my use of County IT resources is subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time. I understand that if my actions result in access to County IT resources from any of my personally owned computing devices (e.g., laptop, home desktop computer, personal digital assistant (PDA), smartphone, cell phone, and USB flash drives), such devices are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time.

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

8. Remote access: I understand that remote access to County IT resources shall require approval by designated County ~~d~~Department ~~County~~ management. If I am authorized to remotely access County IT resources, I shall comply with, and only use equipment that complies with, all applicable County IT resources policies, standards, and procedures, including, without limitation:

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

- Board of Supervisors Policy No. 6.104 – ~~Use of Electronic Mail (email) by County Employee Communications;~~
- Board of Supervisors Policy No. 6.105 – Internet Usage Policy;
- Board of Supervisors Policy No. 6.106 – Physical Security;
- Board of Supervisors Policy No. 6.109 – Security Incident Reporting; and
- Board of Supervisors Policy No. 6.110 – Protection of Information on Portable Computing Devices; ~~antivirus software which is installed and up to date, operating system software and application software which are up to date (e.g., critical updates, security updates, and service packs), and firewall (i.e., software firewall on the computing device or hardware firewall) which is installed and up to date.~~

7.9. Confidentiality: I shall not ~~access, store, or send, disseminate, or otherwise expose or disclose to any person or organization, any personal information, confidential information, and/or other~~ County IT resources (e.g., software code; business data, documentation, and other information; ~~personal data, documentation, and other information; and confidential data, documentation, and other information~~), unless specifically authorized to do so by County management. This includes, without limitation information that is subject to Health Insurance Portability and Accountability Act of 1996, Health Information Technology for Economic and Clinical Health Act of 2009, or any other confidentiality or privacy legislation.

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

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

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

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

~~11.13.~~ Electronic Communications and other information~~mail and other information~~: I understand that County electronic communications (e.g., email, text messages, etc.) created, sent, and/or stored using County electronic communications systems/applications/services are the property of the County. All such ~~, and other information, in either electronic or other forms,~~ electronic communications may be logged/stored, ~~may be are~~ a public record, and are subject to audit and review, including, without limitation, periodic ~~unannounced~~ monitoring and/or investigation, by authorized persons at any time, ~~without notice or consent~~. I shall comply with all County electronic communications email use policies, standards, and procedures and use proper business etiquette when communicating over ~~email~~ County electronic communications systems/applications/services.

~~12. Activities related to County IT resources: I understand that my activities related to County IT resources (e.g., use of email, instant messaging, blogs, electronic files, County Internet services, and County systems) may be logged/stored, are a public record, and are subject to audit and review, including, without limitation, periodic unannounced monitoring and/or investigation, by authorized persons at any time. I do not expect any right to privacy concerning my activities related to County IT resources, including, without limitation, in anything I create, store, send, or receive using County IT resources. I shall not intentionally, or through negligence, damage, interfere with the operation of, or prevent authorized access to, County IT resources and shall use County IT resources responsibly, professionally, ethically, and lawfully.~~

~~13.14.~~ Public forums: Unless I am specifically authorized to do so by designated County Department management as a part of my job function, I shall not use County IT resources to create, exchange, publish, distribute, or disclose in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) not specifically approved by designated County Department management.

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

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

~~16.17.~~ Compliance with County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements: I shall comply with all applicable County ordinances, rules, regulations, policies, procedures, guidelines, directives, and agreements

relating to County IT resources. These include, without limitation, Board of Supervisors Policy No. 6.100 – Information Technology and Security Policy, Board of Supervisors Policy No. 6.101 – Use of County Information Technology Resources, and Board of Supervisors Policy No. 3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

~~17.~~18. Disciplinary action and other actions and penalties for non-compliance: I understand that my non-compliance with any provision of this Agreement may result in disciplinary action and other actions (e.g., suspension, discharge, denial of access, and termination of contracts) as well as both civil and criminal penalties and that County may seek all possible legal redress.

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

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

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

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

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

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

County IT User's Name

County IT User's Signature

County IT User's Employee/ID Number

Date

Manager's Name

Manager's Signature

Manager's Title

Date



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

POLICY

This policy is applicable to all County IT users.

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

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

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

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

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

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

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

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

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

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

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

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

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

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

POLICY

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

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

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

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

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

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

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

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

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

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

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

Definition Reference

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

2009

California Civil Code Section 1798.29

POLICY

This policy is applicable to all County IT users.

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

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

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

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

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

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

Investigations must be notified immediately.

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

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

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

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

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

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

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

Definition Reference

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

[California Civil Code Section 1798.29](#)

POLICY

This policy is applicable to all County IT users.

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

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

- ~~• For any unlawful purpose;~~
 - ~~• For any purpose detrimental to the County or its interests;~~
 - ~~• For personal financial gain;~~
 - ~~• In any way that Must in no way Do not undermine in any way or interferes with the access to or use of County IT resources for official County purposes;~~
 - ~~• In any way that Must Do not hinders in any way productivity, efficiency, or customer service, or interferes in any way with a County IT user's obligation to performance of their-his/her official job duties; or in a timely manner~~
 - ~~• To Neither expresses nor implies sponsorship or endorsement by the County, except as approved by designated County department management; or;~~
 - ~~• For personal purpose where activities are for personal enjoyment, private benefit gain or advantage, or an outside endeavor not related to County business purpose. Personal purpose does not include the incidental and minimal use of County IT resources, such as occasional internet usage, for personal purposes, including an occasional use of the internet.. Any posting to public forums (e.g., newsgroups, chat rooms), or any transmittal of County electronic mail through the Internet for non-business use must include a disclaimer that the views are those of the employee/user and not the County of Los Angeles~~
- ~~— Shall Do not constitute any other access, use, or other activity purpose prohibited by this Board Policy 6.105 result in personal gain (e.g., outside business activities, items for sale)~~

Unless specifically authorized by County ~~Department~~ management or policy, sending, disseminating, or otherwise exposing and/or disclosing any non-public County IT resources information or intellectual property (e.g., software program code; business data, documentation; and or other information; personal data, documentation and or other related information; and any confidential, legislative, or privileged or sensitive data, documentation, and other information) ~~confidential information or personal~~

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

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

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

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

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

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

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

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

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

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

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

Monitoring and/or investigating the access to, and use of, County IT resources by County IT users shall require approval by County management must be approved by management, and conducted in accordance with applicable policies and laws on investigations. If any evidence of violation of this policy abuse is identified, notice shall be provided by County Department management to the Auditor-Controller's Office of County Investigations must be notified immediately.

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

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

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

- Posting or transmitting ~~any message or material which is~~ libelous, ~~or~~ defamatory, fraudulent, or confidential information
- Running/Operating a private business or web site
- Posting or transmitting to unauthorized persons any material deemed to be confidential, ~~information or~~ personal, or otherwise protected from disclosure information
- Participating in partisan political activities
- Attempting ~~an~~ unauthorized access to the account of another person or group on the Internet, or attempting to ~~penetrate beyond~~ circumvent County security measures, ~~or~~ security measures taken by others connected to the Internet, regardless of whether or not such ~~intrusion attempts are successful or~~ results in corruption or loss of data or other information (e.g., password stealing, phishing, or whaling.
- Knowingly or carelessly distributing malicious code to or from County IT resources
- Accessing, creating, or distributing (e.g., via email) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County IT resources (e.g., over County-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless authorized to do so as a part of such County IT user's assigned job function (e.g., law enforcement).

Definition Reference

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Sunset Date: July 13, 2008

Reissue Date:

Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

POLICY

This policy is applicable to all County IT users.

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

Facility Security Plan

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

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

Proper Identification

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

Access to Restricted IT Areas

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

Physical Security Controls

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

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

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

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

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004	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 standards and procedures approved by the Information Security Steering Committee (ISSC) in support of this policy.

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

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

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

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

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

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

Definition Reference

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

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

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

Compliance

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

Policy Exceptions

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

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004
Reissue Date:

Sunset Date: July 13, 2008
Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

POLICY

This policy is applicable to all County IT users.

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

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

Department shall:

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

Definition Reference

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: July 13, 2004

Reissue Date:

Sunset Date: July 13, 2008

Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

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

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

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

Health Insurance Portability and Accountability Act (HIPAA) of 1996

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

[California Civil Code Section 1798.29](#)

POLICY

This policy is applicable to all County IT users.

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

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

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

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

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

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

Chief Information Security Officer (CISO)

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

Examples of these incidents include:

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

Chief HIPAA Privacy Officer

All County IT security incidents that ~~may~~ involve ~~patient p~~ Protected ~~Hh~~ Health ~~i~~ 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 ~~disclosure~~ of patient information

Office of County Investigations (OCI)

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

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

Chief Information Officer (CIO)

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

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

Definition Reference

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

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

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

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

As used in this policy, the term “County IT security” shall have the same meaning as set

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

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

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

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

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

Compliance

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

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007

Reissue Date:

Sunset Review Date: May 8, 2011

Sunset Review Date:



Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

Board of Supervisors Policy No. 6.109 – Security Incident Reporting

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

[Health Insurance Portability and Accountability Act \(HIPAA\) of 1996](#)

[Health Information Technology for Economic and Clinical Health \(HITECH\) Act of 2009](#)

[California Civil Code Section 1798.29](#)

-

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

POLICY

This policy is applicable to all County IT users.

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

A) Portable Computing Devices and Information

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

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

The County prohibits the unnecessary placement (whether by download or, input, or other means) of personal information and/or confidential information on portable computing devices. However, Designated County Department management may authorize specific County IT users to place personal and/or confidential information on portable computing devices if such County IT users must do so as a part of such County IT users' assigned job functions. Prior to authorizing placement on portable computing devices, such County IT users shall who in the course of County business shall must place personal information and/or confidential information on portable computing devices shall be made aware of the risks involved and impact to the affected person/entities in the event of actual or suspected loss or disclosure of personal information and/or confidential information.

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

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

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

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

~~Employee personally procured computing device(s) must adhere to the ISSC approved security and privacy requirements for protection of personal information and/or confidential information when used for County business. Additionally, an Authorization, signed by a designated member of County Department management, shall provide written approval for the particular personal information and/or confidential information to be placed on a portable computing device. The recipient (person using the portable computing device) shall also sign the Authorization to indicate acceptance of the personal information and/or confidential information and to acknowledge his/her understanding of his/her responsibility to protect the information. The Authorization shall be reviewed and renewed, at a minimum, annually. The County Department shall ensure that, in the event the portable computing device is lost or stolen, the County Department shall be able to recreate the personal information and/or confidential information with 100 percent accuracy and shall be able to provide notification to the affected persons/entities.~~

-

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

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

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

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

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

B)C) Personal Information and/or Confidential Limit Exposure of Stored

Information

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

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

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

Definition Reference

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

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

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

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

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

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

As used in this policy, the terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy No. 3.040 –

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

Compliance

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

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007

Reissue Date:

Sunset Review Date: May 8, 2011

Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

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

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

POLICY

This policy is applicable to all County IT users.

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

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

~~countywide~~ information security awareness training program.

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

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

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

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

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

Definition Reference

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

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

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

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: May 8, 2007

Reissue Date:

Sunset Review Date: May 8, 2011

Sunset Review Date:



Los Angeles County BOARD OF SUPERVISORS POLICY MANUAL

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

PURPOSE

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

REFERENCE

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

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

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

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

POLICY

This policy is applicable to all County IT users.

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

Each County Department is responsible for ensuring that all information and software on County-owned or leased computing devices are rendered unreadable and

unrecoverable, whether or not removed from such computing devices, prior to disposition of such computing devices out of County inventory, to prevent unauthorized use or disclosure.

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

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

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

- Computing device sent to salvage
- Computing device destroyed
- Computing device donated to a non-County organization

Definition Reference

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

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

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

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

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

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

Compliance

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

Policy Exceptions

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: October 23, 2007

Reissue Date:

Sunset Review Date: October 23, 2011

Sunset Review Date: