COUNTY OF LOS ANGELES
CHIEF INFORMATION OFFICE
500 West Temple Street
493 Kenneth Hahn Hall of Administration
Los Angeles, CA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008
Facsimile: (213) 633-4733

June 29, 2004

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

Dear Supervisors:

ADOPTION AND APPROVAL OF INFORMATION TECHNOLOGY
AND INFORMATION SECURITY POLICIES
(All Districts) (3 VOTES)

IT IS RECOMMENDED THAT YOUR BOARD:

1. Adopt and approve the attached Information Technology and Security policies.

   a. 6.100 – Information Technology and Security Policy
   b. 6.101 – Use of County Information Technology Resources
   c. 6.102 – Countywide Antivirus Security Policy
   d. 6.103 – Countywide Computer Security Threat Response
   e. 6.104 – Use of Electronic Mail (e-mail) by County Employees
   f. 6.105 – Internet Usage Policy
   g. 6.106 – Physical Security
   h. 6.107 – Information Technology Risk Assessment
   i. 6.108 – Auditing and Compliance

PURPOSE OF RECOMMENDED ACTION

The attached Information Technology and Security Policies have been developed by members of approximately 22 departments under the direction of the Chief Information Office (CIO). The policies provide Board direction for the appropriate use of the County's technology resources and establish minimum operating standards for maintaining security of County technology assets. The completed drafts have been reviewed with all affected parties including Employee Relations (SEIU and the Coalition of Unions), County Counsel, Department Heads and their respective CIOs, Information Systems Steering Committee, Information Systems Commission and your Board

JUSTIFICATION

The recommended Board policies will provide direction to departments, County employees and other users of County information technology (i.e., contractors/consultants) on required practices to be employed in the use of technology.

Publishing these policies will provide a standard for the use of County information technology resources and enforceable sanctions in the event of unauthorized or willful misuse. They also establish minimum security requirements to mitigate against unauthorized access from outside entities (i.e., hackers, viruses, worms, etc.).

FISCAL IMPACT/FINANCING

Adherence to the policies as relates to implementing minimum standards for mitigating security threats will require departments to identify areas of deficiency and develop a corrective action plan. Cost associated with this action will be identified by each department and the CIO will consolidate this information into a countywide security assessment and plan with associated cost. This information will be shared with your Board and the CAO to obtain support for the necessary funding, if it cannot be funded by the respective departments, within their budget.

No financing is required to support these policies.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

Implementation and compliance to Health Insurance Portability and Accountability Act (HIPAA) security rules establish a requirement that covered organizations have security policies. These policies are in concert with these rules.

IMPACT ON CURRENT SERVICES

Approval of the recommended policies will establish the foundation for the effective management and security of information technology assets.

CONCLUSION

We recommend Board approval of the nine (9) policies submitted for adoption.

Respectfully submitted,

JON W. FULLINWIDER
Chief Information Officer

JWF:JW:ygd

Attachments

c: Department Heads
Chair, Information Systems Commission

P:\Drafts\Adoption Approval ITI Security Policies6170419_final.doc

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.100	Information Technology and Security Policy	00/00/00

PURPOSE

To establish a Countywide Information Technology and Security program supported by countywide policies in order to assure appropriate and authorized access, usage and the integrity of County information and information technology assets.

REFERENCE

- Comprehensive Computer Data Access and Fraud Act, California Penal Code 502
- Health Insurance Portability and Accountability Act (HIPAA) of 1996

POLICY

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

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

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

RESPONSIBILITIES

Departments, Commissions, Board and Offices

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

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

Chief Information Office (CIO)

The Office of the CIO will ensure the development of countywide information technology policies that, in addition to security will specify the appropriate use of information technology (I/T) resources for internal and external activities, e-mail and other communications as well as Internet access and use. When approved, these policies will be published and made available to all users of County I/T resources to ensure their awareness and compliance.

Chief Information Security Officer (CISO)

The Chief Information Security Officer reports to the Chief Information Officer (CIO) and is responsible for the I/T Security Program for the County. Responsibilities include:

Developing and maintaining the information security strategy for the County

Chairing the Information Security Steering Committee (ISSC)

Providing information security related technical, regulatory, and policy leadership

Facilitating the implementation of County information security policies

Coordinating information security efforts across departmental lines

Leading information security training and education efforts

Directing the Countywide Computer Emergency Response Team (CCERT)

Departmental Information Technology Management/CIO will:

Manage information technology assets within the Department

Be responsible for any departmental information technology and security policy

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

Ensure that systems are maintained at current critical security patch levels

Implement technology-based services that adhere to the intent and purpose of all information technology use and security policies, standards and guidelines

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

Manage security of information technology assets within the Department

Assist in the development of departmental information technology security policy

Represent the Department at the Information Security Steering Committee (ISSC)

Coordinate the Departmental Computer Emergency Response Team (DCERT)

Employees and Other Authorized Users:

Employees and other department authorized users are responsible for acknowledging and adhering to County information technology use and security policies. They are responsible for protection of County information assets for which they are entrusted and using them for their intended purposes. Employees and authorized non-County users will be required to sign an "Acceptable Use Agreement" as a condition of being granted access to County I/T systems.

Information Security Steering Committee (ISSC)

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

ISSC responsibilities include:

Assisting the CISO in developing, reviewing, and recommending information security policies

Identifying and recommending industry best practices for information security

Developing, reviewing and recommending countywide standards, procedures and guidelines

Coordinating inter-departmental communication and collaboration on security issues

Coordinating countywide I/T security education and awareness

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: **Sunset Date:**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.101	Use of County Information Technology Resources	00/00/00

PURPOSE

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

REFERENCE

Board of Supervisors Policy – Information Technology and Security Policy

Acceptable Use Agreement (Attached)

POLICY

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

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

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

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

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

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

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

Definitions

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

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

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

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

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

- County purchased, licensed, or developed software.

Access Control

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

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

Access control mechanisms may include hardware, software, storage media, policy and procedures, and physical security.

Authentication

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

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

County information technology resource users shall not allow others to access a system while it is logged on under their user sessions. The only exceptions allowed are when the software cannot be configured to enforce a log-in, or where the business needs of the 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 department management.

County information technology resource users shall be responsible for the integrity of the authentication mechanism granted to them. For example, users shall not share their passwords, electronic cards, biometric logons, secure ID cards and/or other authentication mechanisms with others.

Fixed passwords, which are used for most access authorization, must be changed at least every 90 days.

Data Integrity

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

Accessing County Technology Resources Remotely

Access to County technology resources by an employee or non-County employee owned equipment must be approved by department management and/or be part of an approved contract. In all cases, the equipment being used for access must be compliant with County security software requirements.

Privacy

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

Confidentiality

Unless expressly authorized by department management or policy; sending, disclosing, or otherwise disseminating confidential data, protected information, or other confidential information of the County is strictly prohibited. This includes information that is protected under HIPAA or any other privacy legislation.

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contractors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: **Sunset Date:**

Policy #:	Title:	Effective Date:
6.102	Countywide Antivirus Security Policy	00/00/00

PURPOSE

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

REFERENCE

Board of Supervisors Policy – Information Technology and Security Policy.

POLICY

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

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

Each department shall ensure that antivirus software is updated when a new antivirus definition/software release is available and when hardware/software compatibility is confirmed.

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

Each department must comply with the requirements of the CCERT policy in the notification of credible computer threat events.

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

Any employee or authorized user who telecommutes or is granted remote access shall utilize equipment that contains current County-approved anti-virus software and shall adhere to County hardware/software protection standards and procedures that are defined for the County and the authorizing department.

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

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

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

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contractors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: **Sunset Date:**

Policy #:	Title:	Effective Date:
6.103	Countywide Computer Security Threat Response	00/00/00

PURPOSE

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

REFERENCE

Board of Supervisors Policy – Information Technology and Security Policy.

POLICY

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

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

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

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

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

Each department shall provide CCERT with after hours contact information for their primary and secondary representatives. Each department shall maintain current contact information for all personnel who are responsible for managing I/T resources to be utilized to remediate security threats.

Departments shall provide primary and secondary members with adequate portable communication devices. (e.g., cell phone, pager, etc).

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: **Sunset Date:**

Policy #:	Title:	Effective Date:
6.104	Use of Electronic Mail (e-mail) by County Employees	00/00/00

PURPOSE

To ensure that all County e-mail communications are used in accordance with applicable laws and County Use of Information Technology Policies. This policy also requires that electronic mail systems be secured to prevent unauthorized access, to prevent unintended loss or malicious destruction of data, and to provide for their integrity and availability.

REFERENCE

Board of Supervisors Policy – Information Technology and Security Policy

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

POLICY

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

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

All e-mail messages are the property of the County and subject to review by authorized County personnel. Staff cannot expect a right to privacy when using the County e-mail system.

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

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

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

Internet based e-mail services shall not be accessed using County information technology resources except for County purposes.

E-mail retention must comply with legal requirements, but must be minimized to conserve information technology resources and prevent risk of unauthorized disclosure.

Encryption of e-mail may be appropriate or required in some instances to secure the contents of an e-mail message.

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contractors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: **Sunset Date:**

Policy #:	Title:	Effective Date:
6.105	Internet Usage Policy	00/00/00

PURPOSE

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

REFERENCE

Board of Supervisors Policy – Information Technology and Security Policy.

POLICY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contractors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: **Sunset Date:**

Policy #:	Title:	Effective Date:
6.106	**Physical Security**	00/00/00

PURPOSE

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

REFERENCE

Board of Supervisors Policy – Information Technology and Security Policy.

POLICY

Facility Security Plan

Each County department is required to have a "Facility Security Plan" which shall include measures to safeguard Information Technology resources. The plan shall describe ways in which all Information Technology resources shall be protected from physical tampering, damage, theft, or unauthorized physical access.

Proper Identification

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

Access to Restricted IT Areas

Restricted I/T areas including data centers, computer rooms, telephone closets, network router and hub rooms, voicemail system rooms, and similar areas containing I/T resources. All access to these areas must be authorized and restricted.

Equipment Control

The assigned user of I/T resource is considered the custodian for the resource. If the item has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, the custodian must promptly inform the involved department manager.

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

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

Compliance

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as civil and criminal penalties. Non-employees including contractors may be subject to termination of contractual agreements, denial of access and/or penalties both criminal and civil.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: **Sunset Date:**

Policy #:	Title:	Effective Date:
6.107	Information Technology Risk Assessment	00/00/00

PURPOSE

To ensure the performance of periodic countywide and departmental information security risk assessments for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

REFERENCE

Board of Supervisors Policy – Information Technology and Security Policy

POLICY

Security risk assessment is a mandatory activity, which encompasses information gathering, analysis, and determination of security vulnerabilities within the County's hardware and software environment, and information technology (I/T) business practices.

Security risk assessment is necessary to analyze and mitigate threats to the County information technology assets, which may come from any source including natural disasters, disgruntled employees, hackers, the Internet, equipment or service malfunction or breakdown.

Security risk assessments shall be conducted on all information systems including applications, servers, networks, and any process or procedure by which these systems are utilized and maintained. Risk assessment shall also be performed on facilities that house information technology resources.

A risk assessment program shall include an inventory of I/T assets, review of I/T policy and procedures, assessments and prioritization of data security vulnerabilities, and implementation of safeguards to mitigate identified vulnerabilities.

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

Compliance

County departments must develop written procedures to comply with this policy. Review and remediation of risk assessment findings is the responsibility of each department.

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: **Sunset Date:**

Policy #:	Title:	Effective Date:
6.108	Auditing and Compliance	00/00/00

PURPOSE

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

REFERENCE

Board of Supervisors Policy – Information Technology and Security Policy.

POLICY

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

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

Compliance

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

Policy Exceptions

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

RESPONSIBLE DEPARTMENT

Chief Information Office (CIO)

DATE ISSUED/SUNSET DATE

Issue Date: **Sunset Date:**