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

May 8, 2007

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 SECURITY POLICIES
(All Districts) (3 Votes)

IT IS RECOMMENDED THAT YOUR BOARD:

1. Adopt and approve attached Information Technology and Security policies:
   a. 6.109 – Security Incident Reporting Policy
   b. 6.110 – Protection of Information on Portable Computing Devices Policy
   c. 6.111 – Information Security Awareness Training Policy

2. Approve Pointsec encryption software as the standard security software for full disk encryption for County laptop computers.

3. Approve designated funds in the amount of $791,136 from the Information Technology Fund (ITF) to acquire 12,550 encryption software licenses, first year maintenance and support, and implementation services for deployment in County departments.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

The attached Information Technology (IT) and Security policies have been developed and approved by the County's Information Security Steering Committee comprised of all County departments. The completed drafts have been reviewed by department management and other affected parties including Employee Relations (Service Employee International Union and Coalition of County Unions), County Counsel, Information Systems Commission, the Audit Committee, and your Board IT Deputies.

These policies are designed to enhance the County's information security program and to improve the protection of County sensitive/confidential information. Additionally, they will provide Board direction for employee security incident reporting, protection of sensitive information on portable computing devices, and security awareness.

Security Incident Reporting Policy (6.109)

The Security Incident Reporting Policy (Attachment A) identifies notification and reporting requirements for all IT-related security incidents, including the need to notify individuals whose personal information may have been compromised.

Protection of Information on Portable Computing Devices Policy (6.110)

The Protection of Information on Portable Computing Devices Policy (Attachment B) requires that all County laptop computers have full disk encryption to protect any and all information that is contained on them. It also requires that management approve the downloading of personal and/or confidential information to portable devices and that the information be encrypted regardless of the type of portable device. To meet the requirements of this policy, the County must purchase encryption software that can be used on all laptop computers.

Selection of Pointsec Encryption Software

To identify and select an encryption solution, the Chief Information Office (CIO) coordinated with all County departments and developed a Request for Proposal (RFP) to competitively solicit, evaluate and acquire the necessary software. Pointsec was selected after a competitive evaluation as having the best solution for meeting the County's requirements. In recommending the acquisition of Pointsec encryption software, we are also recommending that the Board adopt this solution as the County standard until such time that it is determined a better product solution is available.

We have negotiated with Pointsec for enterprise pricing to acquire 12,550 encryption software licenses and implementation services for deployment on all laptop and selected desktop devices. We are requesting Board approval of designated funds in the amount of $791,136 from the Information Technology Fund (ITF) to support this effort. Subsequent year funding for annual maintenance and additional devices beyond the initial purchase will be the responsibility of the departments. Those departments that have funding or a source of funding will be required to reimburse the Information Technology Fund.

Information Security Awareness Training Policy (6.111)

The Information Security Awareness Training Policy (Attachment C) requires that all departments conduct periodic training for all users of County IT resources. This includes basic security awareness as well as policy requirements in the protection of IT assets entrusted to and possessed by employee and/or contractor(s) in the performance of County duties.

Implementation of Strategic Plan Goals

The recommendations support the County Strategic Plan Goals of Service Excellence, Workforce Excellence, Organization Effectiveness, and Fiscal Responsibility. The County processes and maintains large amounts of sensitive and confidential information to serve its constituents. These recommendations will enhance the County's information security program and will establish appropriate safeguards used to protect personal and confidential information.

FISCAL IMPACT/FINANCING

Implementation of the portable computing device protection policy will require that the County acquire encryption software and install it on designated portable devices. Completion of this process is a high priority and will require ITF funds in the amount of $791,136 to acquire encryption software licenses and implementation services for initial deployment in County departments. Those departments that have funding or a source of funding will be required to reimburse the Information Technology Fund.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

County Code Section 2.119.03(C) provides that the Office of the CIO shall "Adopt standards for countywide information technology, which shall be subject to approval by the Board of Supervisors. County departments and County information technology bodies shall adhere to such standards."

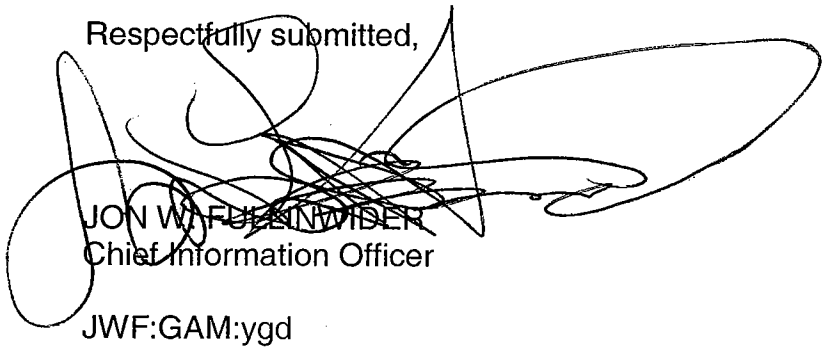
IMPACT ON CURRENT SERVICES (OR PROJECTS)

The approval of these recommended policies and the funds for the initial deployment of encryption software will enhance the County's information security program and will establish appropriate safeguards used to protect personal and confidential information.

CONCLUSION

Approval of the attached policies will enhance the County's information security program and will establish appropriate safeguards used to protect personal and confidential information. The approval of ITF funds will enable departments to effectively implement the IT Security policy regarding Protection of Information on Portable Computing Devices (6.110) by supporting the acquisition and deployment of encryption software in County departments.

Respectfully submitted,



JON W. FULLINWIDER
Chief Information Officer

JWF:GAM:ygd

Attachments

c: Department Heads
Information Systems Commission

P:\CISO Activities\Encryption Portable Devices\ITF And Board Notice\bosinfosecuritypolicies50107_bdltr R2.doc

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.109	**Security Incident Reporting**	00/00/00

PURPOSE

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

REFERENCE

Board of Supervisors Policy #3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information
Board of Supervisors Policy #6.100 – Information Technology and Security Policy
Board of Supervisors Policy #6.101 - Use of County Information Technology Resources
Board of Supervisors Policy #6.103 - Countywide Computer Security Threat Responses
Board of Supervisors Policy #6.110 - Protection of Information on Portable Computing Devices

POLICY

All information technology (IT) related security incidents (i.e., virus/worm attacks, actual or suspected loss or disclosure of personal and/or confidential information, etc.) must be reported to the applicable designated County offices in a timely manner to minimize the risk to the County, its employees and assets, and other persons/entities. The County department that receives a report of an incident must coordinate the information gathering and documenting process and collaborate with other affected departments to identify and implement a resolution or incident mitigation action (i.e., notification of unauthorized disclosure of personal and/or confidential information to the affected employee and/or other person/entity, etc).

In all cases, IT related security incidents must be reported by the Chief Information Office (CIO) to the Board of Supervisors (Board) delineating the scope of the incident, impact, actions being taken and any action taken to prevent a further occurrence. Board notification must occur as soon as the incident is known. Subsequent updates to the Board may occur until the incident is closed as determined by the Chief Information Security Officer (CISO).

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

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

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

HIPAA Privacy Officer (HPO)
All IT related security incidents that may involve patient protected health information (PHI) must be reported by the affected County departments to the HPO. 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 disclosure of patient information

Office of County Investigations (OCI)
All IT related security incidents that may involve non-compliance with any Acceptable Usage Agreement (Refer to Board of Supervisors Policy #6.101, Use of County Information Technology Resources) or the actual or suspected loss or disclosure of personal and/or confidential information must be reported to OCI. These incidents can be reported using an on-line form found at www.lacountyfraud.org. Examples of these incidents include:

- System breaches from internal or external sources
- Lost or stolen computers and data
- Inappropriate non-work related data which may include pornography, music, videos
- Actual or suspected loss or disclosure of personal and/or confidential information

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

suspected loss or disclosure of personal and/or confidential information, and final actions taken to mitigate and prevent future occurrences of similar events.

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

Definition Reference
As used in this policy, the terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy #3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

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

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: Month XX, 2007 **Sunset Date:**

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.110	**Protection of Information on Portable Computing Devices**	00/00/00

PURPOSE

To establish a policy regarding the protection of personal 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

Board of Supervisors Policy #3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information
Board of Supervisors Policy #6.100 – Information Technology and Security Policy
Board of Supervisors Policy #6.109 - Security Incident Reporting
Authorization to Place Personal and/or Confidential Information on a Portable Computing Device (attached)

POLICY

This policy is applicable to all County departments, employees, contractors, sub-contractors, volunteers and other governmental and private agency staff who use portable computing devices in support of County business.

Definition Reference

As used in this policy, the terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy #3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

Placing Personal and/or Confidential Information On Portable Computing Devices

The County prohibits the unnecessary placement (download or input) of personal and/or confidential information on portable computing devices! However, users who in the course of County business must place personal and/or confidential information on portable

computing devices must be made aware of the risks involved and impact to the affected persons/entities in the event of actual or suspected loss or disclosure of personal and/or confidential information. If personal and/or confidential information is placed on a portable computing device, every effort must be taken, including, without limitation, physical controls, to protect the information from unauthorized access and, without exception, the information must be encrypted. Additionally, a written authorization signed by a designated member of departmental management must provide written approval for the particular personal and/or confidential information to be placed on a portable computing device. The recipient (person using the portable computing device) must also sign the authorization indicating acceptance of the information and acknowledge his/her understanding of his/her responsibility to protect the information. The authorization must be reviewed and renewed, at a minimum, annually. In the event the portable computing device is lost or stolen, the department must be able to recreate the personal and/or confidential information with 100 percent accuracy and must be able to provide notification to the affected persons/entities.

Full Encryption of All Information on all Portable Computing Devices

Security measures must be employed by all County departments to safeguard all personal and/or confidential information on all portable computing devices. All County-owned or provided portable computers (e.g., laptops and tablet computers) must at all times have automatic full disk encryption that does not require user intervention nor allow user choice to implement. If personal and/or confidential information is placed on any portable computing devices, all such information must be encrypted while on those portable computing devices.

Portable computing devices include, without limitation, the following:

- Portable computers, such as laptops and tablet computers
- Portable devices, such as personal digital assistants (PDA), digital cameras, portable phones, and pagers
- Portable storage media, such as diskettes, tapes, CDs, zip disks, DVDs, flash memory/drives, and USB drives

If personal and/or confidential information is stored on a portable computing device, it is the department's responsibility to ensure that the portable computing device supports department approved data encryption software and that all information is encrypted that resides on this device.

Personal and/or Confidential Information

When it is determined that personal and/or confidential information must be placed on a portable computing device, every effort should be taken to minimize the amount of information required. Additionally, if possible, information should be abbreviated to limit exposure (e.g., last 4 digits of the social security number).

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

Any actual or suspected loss or disclosure of personal and/or confidential information must be reported under Board of Supervisors Policy 6.109, Security Incident Reporting. In all cases, every attempt must be made to assess the impact of storing, and to mitigate the risk to, personal and/or confidential information on all portable computing devices.

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

There are no exceptions to this policy.

RESPONSIBLE DEPARTMENT

Chief Information Office

DATE ISSUED/SUNSET DATE

Issue Date: Month XX, 2007 **Sunset Date:**

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

Department Name _____

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

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

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

Portable Computing Device Description:

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

Device serial number: _____

Property number (if County property): _____

Name of encryption software installed: _____

Operating system: _____

Information Being Placed on the Portable Computing Device:

Purpose of placement: _____

Application system name (if applicable): _____

Personal and/or confidential information fields: _____

_____

_____

_____

_____

_____

User Agreement and Acknowledgement:

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

Name: _____ Date: _____

Signature: _____

Department Approval:

Print Name: _____ Title: _____

Signature: _____

Los Angeles County
BOARD OF SUPERVISORS POLICY MANUAL

Policy #:	Title:	Effective Date:
6.111	**Information Security Awareness Training**	00/00/00

PURPOSE

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

REFERENCE

Board of Supervisors Policy #3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information
Board of Supervisors Policy #6.100 – Information Technology and Security Policy

POLICY

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

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

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

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

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

Definition Reference

As used in this policy, the terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy #3.040 – General Records Retention and Protection of Records Containing Personal and Confidential Information.

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

DATE ISSUED/SUNSET DATE

Issue Date: Month xx, 2007 **Sunset Date:**