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

May 8, 2007, Board Order No. 26

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

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

Placing Personal and/or Confidential Information On Portable Computing Devices

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

Full Encryption of All Information on all Portable Computing Devices

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

Portable computing devices include, without limitation, the following:

• Portable computers, such as laptops and tablet computers

• Portable devices, such as personal digital assistants (PDA), digital cameras, portable phones, and pagers

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

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

Personal and/or Confidential Information

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

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

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

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: May 8, 2007 **Sunset Review Date: May 8, ~~2011~~2015**

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: _____