County of Los Angeles
CHIEF ADMINISTRATIVE OFFICE
713 KENNETH HAHN HALL OF ADMINISTRATION • LOS ANGELES, CALIFORNIA 90012
(213) 974-1101
http://cao.co.la.ca.us

DAVID E. JANSSEN
Chief Administrative Officer

October 3, 2006

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:

POLICY #3.040 GENERAL RECORDS RETENTION AND PROTECTION OF RECORDS CONTAINING PERSONAL AND CONFIDENTIAL INFORMATION (ALL DISTRICTS AFFECTED) (3 VOTES)

IT IS RECOMMENDED THAT YOUR BOARD:

1. Approve revised Policy #3.040 General Records Retention and Protection of Records Containing Personal and Confidential Information to establish guidelines for retaining records, describe personal and confidential information and steps to protect such data, and mandate safeguards for the destruction of confidential records.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

On February 28, 2006, your Board instructed the Chief Administrative Office (CAO) to update the County Policy Manual to address appropriate securing and prompt disposal of confidential records, papers, or documents, and ensure that all County departments come into compliance.

Subsequently, on May 2, 2006, your Board directed this Office, the Chief Information Officer (CIO), and the Directors of Personnel and Consumer Affairs to review existing County policies pertaining to the storage and portability of confidential employment records in order to assess the potential for breach and/or unauthorized use. Additionally, the CIO, Auditor-Controller, and Directors of Community and Senior Services, Consumer Affairs, and Personnel, with oversight by the CAO, were directed to report back with recommendations to improve the security of confidential employee, and other individual, records.

On August 17, 2006 this Office and CIO presented a set of policies responsive to these Board orders to the Audit Committee. The Audit Committee recommended approval of these policies by your Board. The policies developed by the CIO relative to the storage and portability of confidential employment records on portable devices will be separately submitted to your Board by the CIO for approval. The attached Policy #3.040 General Records Retention and Protection of Records Containing Personal and Confidential Information is submitted for your approval.

It should be noted that departments may develop additional policies and procedures that are stricter than the parameters set forth in Policy #3.040 in order to safeguard protected health information as may be required under State and Federal laws, specifically Health Insurance Portability and Accountability Act (HIPAA).

Implementation of Strategic Plan Goals

The approval of Policy #3.040 will provide employees with protocols in handling records containing personal and confidential information. Therefore, the proposed policy is consistent with the County Strategic Plan Goals of Service Excellence and Organizational Effectiveness.

FISCAL IMPACT/FINANCING

Departments are currently maintaining, storing, and disposing of records; as such, compliance with the revised policy should have minimal fiscal impact.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

As a result of two reported incidents of potential security breaches relative to confidential employee records and client information maintained by County departments, your Board directed this Office to update the County Policy Manual to address appropriate securing and prompt disposal of confidential records, papers, or documents. The CAO, CIO, Auditor-Controller, and Directors of Community and Senior Services, Consumer Affairs, and Personnel have worked together and the following items have been prepared in response to your Board's instructions:

Outreach Programs - Consumer Affairs, as reported to your Board April 28, 2006, developed outreach strategies on identity fraud for County employees and residents.

Policy for Portable Computing Devices - The CIO undertook development of several policies to ensure appropriate use and applicable safeguards for protecting confidential information on portable computing devices, as well as appropriate training. Such policies will be separately submitted to your Board by the CIO for approval.

Policy for Handling Confidential Information - This Office developed the attached Policy which has been approved by the Audit Committee. The CAO will work with County departments to ensure compliance with the attached policy by conducting a presentation to Administrative Deputies, as well as the County Records and Archives Coordinators.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

The revised policy provides employees with defined protocols in handling records containing personal and confidential information. The policy addresses record retention, protection of records

containing personal or confidential information, destruction of records containing personal or confidential information, and confidential information incident reporting. There are no exceptions to the proposed policy, which is summarized below:

Record Retention - County departments are to comply with the policy guidelines provided for records retention and specific procedures pertaining to the protection of records containing personal or confidential information. The guidelines will remain in place until your Board approves the General Retention Schedules for common administrative records which will be applicable to all County departments, as well as Retention Schedules specific to the records maintained by individual departments.

Protection of Records - Describes personal and confidential information and identifies steps County departments must take to protect these records, including restricting access to such records by authorized personnel only.

Destruction of Records - Describes methodology for the destruction of records containing personal or confidential information. Mandatory safeguards are also included. The goal is for departments to destroy information completely to ensure that the information cannot be recognized or reconstructed. Personal or confidential data stored on computer media must be obliterated and/or made indecipherable before disposal.

Respectfully submitted,

DAVID E. JANSSEN
Chief Administrative Officer

DEJ:MKZ
DS:MLM:pg

Attachment

c: All Department Heads

Policy #:	Title:	Effective Date:
3.040	General Records Retention and Protection of Records Containing Personal and Confidential Information	05/13/58

PURPOSE

Provides general guidelines to be followed by departments in the retention and destruction of records and specific procedures for the protection of records containing personal and confidential information.

REFERENCE

May 13, 1958 Board, Order, Synopsis 46
February 28, 2006 Board Order, Synopsis 23-A
May 2, 2006 Board Order, Synopsis 3
Government Code Section 26202
Policy #6.100: Information Technology and Security
Policy #6.106: Information Technology Physical Security
Policy #6.107: Information Technology Risk Assessment
Policy # 6.109 *(Tentative)*: Security Incident Reporting
Policy # 6.110 *(Tentative)*: Protection of Information on Portable Computing Devices
Policy # 6.111 (*Tentative*): Information Security Awareness Training

POLICY

County departments are to comply with the following general guidelines on records retention and specific procedures pertaining to protection of records containing personal or confidential information pending 1) Board of Supervisors' approval of the General Retention Schedules for common administrative records, which will be applicable to all County departments; and 2) Board of Supervisors' approval of the Retention Schedule specific to the records maintained by a particular department. Thereafter, each department must follow the General Retention Schedules; its specific Retention Schedule; and any policies and procedures approved by the Board of Supervisors regarding records management practices.

Records Retention - Generally

County departments shall retain records that are useful and/or are required by law (including State or Federal law) to be filed and preserved. However, County departments may destroy any record, paper or document that:

1. Is more than two years old;
2. Is of no further use to the department;
3. Is not expressly prepared or received pursuant to State statute or County charter; and
4. Is not expressly required by any law (including State or Federal law) to be filed and preserved.

Protection of Records Containing Personal or Confidential Information

County departments shall secure and appropriately dispose of all records, papers or documents with personal or confidential information.

Confidential information is information that is sensitive, proprietary or personal to which access must be restricted and whose unauthorized disclosure could be harmful to a person, process or to an organization.

Personal information is any information maintained by a department that identifies or describes an individual including, but not limited to, his or her name, social security number, physical description, home address, telephone number, education, financial matters, and medical or employment history.

Paper documents that contain personal or confidential information such as social security numbers, health-related information, or financial information must be properly stored and secured from view by unauthorized persons.

Security measures must also be employed by all departments to safeguard personal or confidential data contained on all information technology assets in the custody of the County.

(See also Board of Supervisors Policies 6.100 Information Technology and Security, 6.106 Information Technology Physical Security, 6.107 Information Technology Risk Assessment and 6.110 (Tentative), Portable Computing Device Security.)

Departments must ensure that only authorized personnel may hold and have access to such information.

Destruction of Records Containing Personal or Confidential Information:

When records containing personal or confidential information are ready for destruction, departments shall destroy the information completely to ensure that the information cannot be recognized or reconstructed. In addition, any personal or confidential data contained on computer media must be obliterated and/or made indecipherable before disposing of the tape, diskette, CD-ROM, zip disk, or other type of medium.

Each department must provide appropriate methods and equipment to routinely destroy personal or confidential information. The safeguards listed are in priority order with the most highly recommended safeguard listed first. At the minimum, one of the following safeguards must be implemented:

- Conduct due diligence and hire a document destruction contractor to dispose of material either offsite or onsite.
    - Require that the disposal company be certified by a recognized trade association.
    - Review and evaluate the disposal company's information security policies and procedures.
    - Review an independent audit of a disposal company's operations and/or its compliance with operations.
- Secure and utilize shredding equipment that performs cross-cut or confetti.
- Secure and utilize erasing equipment.
- Modify the information to make it unreadable or indecipherable through any means.

Confidential Information Incident Reporting

Each department must disclose to the department's management and the designated security officer any actual or suspected incident in which confidential information is disclosed to, or obtained by, an unauthorized person. Notification of the security incident must be made in the most prompt and expedient manner after the incident has been discovered. In addition, any such incident must be reported to the Fraud Hotline at 800.544.6861 or the Auditor-Controller's Office of County Investigations website at www.lacountyfraud.org where protocols are in place to respond to the incident.

Within ten days, a letter notifying affected individuals of actual or suspected loss or disclosure of personal or confidential information must be sent by the impacted County department describing the types of information lost and recommended actions to be taken to mitigate the potential misuse of their information

The Chief Information Security Officer must also be promptly informed of the security breach associated with electronic data in order to communicate with other County departments and identify appropriate measures and safeguards.

(See also Board of Supervisors Policy 6.109 (Tentative): Security Incident Reporting, and 6.111 (Tentative): Information Security Awareness Training.)

Policy Exceptions

There are no exceptions to this policy.