COUNTY OF EL DORADO, CALIFORNIA
BOARD OF SUPERVISORS POLICY

Subject:	Policy Number	Page Number:
COMPUTER and DATA SYSTEMS PHYSICAL SECURITY	A-17	1 of 5
	Date Adopted: 06/17/1997	Revised Date: 11/15/2005

PURPOSE:

To establish a policy to set forth reasonable and enforceable standards for the protection, security, and availability of County data in the event of storage media failure or Data Center disaster.

BACKGROUND:

This document supports the El Dorado County COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY (Policy A-13).

DEFINITIONS:

Physical Security – Measures to physically protect the County's data and information assets; e.g. data stored on PC's, servers, storage devices, lock and key systems, electronic access control systems, and electronic surveillance systems.

Logical Security – Automated procedures taken to protect the County's assets, e.g. user identifiers, passwords, file access control.

Operating System Software – Computer programs used to control the operation of the computers and peripheral equipment, including telecommunication equipment. These computer programs are also called systems software.

Data Center Disaster – The El Dorado County Data Center is located at 360 Fair Lane in the lower level of Building B. A disaster in this facility is defined as any event that renders a majority

of the equipment in the Data Center unavailable or unusable, affecting County mission-critical applications and systems, for a period longer than 72 hours.

Storage Media Failure – Most of the data stared in the Data Center is recorded electronically on various types of disk and tape storage devices. A failure of one of these devices can result in the data being lost because the surface of the disk may become unreadable.

POLICY:

It is the policy of the Board of Supervisors that the County's data be processed in a secure environment. The cost of security, including the testing of security plans and safeguards, should be commensurate with the value of the data, considering value to the data owner/user, the data subject and the potential data abuser.

Further, it is the policy of the of the Board of Supervisors that, with respect to the processing and storage of County data, measures be taken to ensure against the unauthorized modification, destruction, or disclosure of confidential data, whether accidental or intentional. Also measures are to be taken to ensure the ability to recover and restore data files in the event of a storage media failure or the destruction of the County's Data Center. In the event of a Data Center disaster plans must be in place to restore operations within seven days and files should be restored to a status reflecting that as of the close of business seven days prior to the destruction event. In the event of media failure, data files should be restored to a status reflecting that of the close of the previous business day.

The Board of Supervisors recognizes that most records kept by the County are by their nature public records available to the public unless a specific statutory provision authorizes the County to withhold a public record from public disclosure. This policy shall be interpreted in conformance

to case and statutory law relating to public records, and it is further recognized that such laws are applicable even though public records are stored in a computer.

It is the policy of the Board of Supervisors that it shall be the responsibility of a department, or agency to identify those such records which may be withheld from public disclosure based upon statutory authority, state or federal. It is also the policy of the Board that a department or agency shall identify those individuals with a need to access such non-public records.

Under direction of this policy, the responsibilities as shared by IT and user agencies and departments for protection, security and availability of mainframe data processed by El Dorado County are:

Information Technologies (IT)

1. Provide physical security for data and computing resources in its custody;

2. Provide control consistent with this policy over access to data;

3. Develop, maintain and test a backup and recovery plan consistent with this policy to ensure restoration of data files and continuity of operations in the event of a Data Center disaster or media failure;

4. Provide logical security features for protecting data resources;

5. Provide security for operating system software and its associated data;

6. Inform the users of the availability, capabilities, and weaknesses of security features;

7. Inform the users of any change, in hardware, operating system software, or other features, which could affect data security;

8. Report in a timely manner any detected unauthorized actions affecting the users' data to the appropriate user management;

9. Include data security requirements in feasibility studies;

10. IT will work with user departments to ensure that they:

    a. Provide physical security for data and computing resources in their custody;

    b. Identify and classify sensitive data;

    c. Identify authorized users of the data;

    d. Identify the potential risk associated with the loss or destruction of data;

    e. Ensure that measures are implemented by IT, systems developers and users of data to provide the required level of data security.

11. IT shall maintain the necessary environmental systems in the data center to ensure proper operating temperature and humidity levels for all equipment located therein.

It is also the policy of the Board of Supervisors that individual employees be given computer user ID's and that these ID's be associated with passwords chosen by the employee and changed at regular intervals by the employee, Employees are not to share or reveal these passwords with others and are not to use another employee's user ID and password or allow another employee to use their user ID and password. Violation of these policies may result in disciplinary action up to and including termination.

Primary Department: Information Technologies

References: None