COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

Subject:	Policy Number:	Page Number:
DATA CENTER AND NETWORK SYSTEMS PHYSICAL SECURITY	A-17	1 of 1
	Date Adopted: XX/XX/XXXX	Effective Date: XX/XX/XXXX

I. PURPOSE

The purpose of this policy is to:

A. Establish a policy to set forth reasonable and enforceable standards for the physical protection, security, and availability of County data.

II. POLICY

A. The County's data shall be processed in a secure environment. The cost of security, including the testing of security plans and safeguards, shall be commensurate with the value of the data, considering value to the data owner/user, and the data subject.

B. Measures shall be taken with respect to the processing and storage of County data to ensure against the unauthorized modification, destruction, or disclosure of confidential data, whether accidental or intentional. Also measures shall be taken to ensure the ability to recover and restore data files in the event of a media failure or the destruction of the County's data center. In the event of a data center disaster, a Continuity of Operations Plan (COOP) must be in place to restore critical operations within seven days and files shall 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 (i.e. data array), data files shall be restored to a status reflecting that of the close of the previous business day.

C. 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.

D. It shall be the responsibility of the County Department or Agency to identify those records that may be withheld from public disclosure, based upon statutory authority, state or federal regulations. Additionally, the Department or Agency shall identify those individuals with a need to access such non-public records.

III. **PROCEDURE**

The Information Technologies Department (IT), user Departments and Agencies shall share the following responsibilities for protection, security and availability of data processed by El Dorado County:

A. Provide physical security for data and computing resources in the Department or Agency's custody:

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

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

   c. IT in collaboration with Facilities Maintenance shall maintain the necessary environmental systems in the data center to ensure proper operating temperature and humidity levels for all equipment located therein in accordance with Code of Federal Regulations Title 45, Section 164.310 – Physical Safeguards, as required to be in compliance with Protected Health Information (PHI) regulations;

   d. IT in collaboration with Facilities will ensure proper physical security of the data center in accordance with Code of Federal Regulations 45, Section 164.310. Access to network equipment housed at all County-occupied sites should remain locked at all times, and entry by authorized staff should be by means of an electronic key card system. In the case where electronic key cards are not available or currently installed, doors are to remain locked and physical keys are to be used.

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

   a. 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.

C. Include data security requirements in feasibility studies;

   a. Report in a timely manner any detected unauthorized actions affecting the users' data to the appropriate user Department or Agency management, as well as to the Risk Management Division of the Human Resources Department;

b. Follow protocols referenced in the IT Data Breach Response Procedure, as noted in the General Network Usage Procedures and Guidelines document.

D. 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 (as specified by the user department);

c. Identify authorized users of the data (as specified by the user department);

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 to be in compliance with user department specified regulations;

f. Allow authorized personnel only to the data center for which they are responsible, to perform specific tasks with respect to the installation, maintenance, auditing, and decommissioning of equipment housed there;

g. Inform the users of the availability, capabilities, and potential threats or risks of hosted applications.

IV. REFERENCES

NIST Publication 800-53 rev. 4, Board Policy A-19 General Network Usage Policy, Code of Federal Regulations Title 45 Part 164, IT Data Breach Response Procedure.

V. RESPONSIBLE DEPARTMENT

Information Technologies

VI. DATES ISSUED AND REVISED; SUNSET DATES:

Issue Date:	XX/XX/XXXX	Sunset Review Date:	XX/XX/XXXX
Revision Date:	XX/XX/XXXX	Sunset Review Date:	XX/XX/XXXX