COUNTY -OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

Subject:	Policy Number:	Page Number:
~~COMPUTER AND DATA~~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. ~~A.~~ To establish a policy to set forth reasonable and enforceable standards for the physical 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.~~

II. POLICY

A. ~~It is the policy of the Board of Supervisors that ~~T~~t~~he County's data shall be processed in a secure environment. The cost of security, including the testing of security plans and safeguards, shall~~should~~ be ~~be~~ commensurate with the value of the data, considering value to the data owner/user, ~~-~~and the data subject ~~and the potential data abuser~~.

B. ~~-~~Measures shall be taken ~~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~~-~~ shall be ~~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 d~~D~~ata c~~C~~enter. In the event of a d~~D~~ata c~~C~~enter disaster, a~~the~~ Continuity of Operations Plan ~~C~~(COOP) ~~(continuity of operations plan)plans~~ must be in place to restore critical operations within seven days and files shall~~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 (i.e. data array), data files shall~~should~~ be restored to a status reflecting that of the close of the previous business day.

C.

~~C. The Board of Supervisors recognizes that~~ M~~m~~ost 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 ~~It is the policy of the Board of Supervisors that it~~ shall be the responsibility of ~~a~~ the County D~~d~~epartment~~,~~ or A~~a~~gency ~~-~~to identify ~~those such~~those records that~~which~~ may be withheld from public disclosure, based upon statutory authority, state or federal regulations. Additionally, t~~T~~he ~~-It is also the policy of the Board that a~~ D~~d~~epartment or A~~a~~gency shall identify those individuals with a need to access such non-public records.

~~E. Under the 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:~~

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. ~~A.~~ Provide physical security for data and computing resources in the Department or Agency's~~its~~ 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 Maintenanc~~e~~e 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~~ Regulations Title 45, Section 164.310 – Physical Safeguards, as required to be in compliance with Protected Health Information (PHI) regulations.~~.~~

~~a.~~d. ~~Along with the environmental controls, the~~ IT in collaboration with ~~department and~~ Facilities will ensure proper physical security of the data center in accordance with Code of Federal Regulations 45, Section 164.310.~~,~~ Access to ~~Physical security of~~ n~~n~~etwork equipment housed at all County-~~-~~occupied sites should remain locked at all times, and~~.~~ e~~E~~ntry 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. ~~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 d~~D~~ata c~~C~~enter 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~~to~~ Risk Management Division of the Human Resources Department ~~in a timely manner any detected unauthorized actions affecting the users' data to the appropriate user management;~~

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

~~(Jimmy) add protocol for reporting breaches – (Possible MS-ISAC established procedures)~~

~~C. 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;~~

D. ~~IT staff~~~~Authorized personneler~~~~Provide logical security features for protecting data resources;~~

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

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

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

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

~~I. Include data security requirements in feasibility studies;~~

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

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

~~b.~~a.

~~c.~~ Identify and classify sensitive data (as specified by the user department);

~~d.~~b.

~~e.~~ ~~identify~~ Identify authorized users of the data (as specified by the user department);

~~f.~~c.

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

~~h.~~d.

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 a~~A~~uthorized personnel only ~~are only permitted entry~~ to the data center for which they are responsible, ~~in order~~ to ~~undertake~~perform specific tasks with respect to the installation, maintenance, auditing, and decommissioning of equipment housed there ~~and for which they have responsibility~~;

- Inform the users of the availability, capabilities, and potential threats or risks of hosted applications;

g.

~~K. IT shall maintain the necessary environmental systems in the data center to ensure proper operating temperature and humidity levels for all equipment located therein. Along with the environmental controls, the IT department and Facilities will ensure proper physical security of the data center in accordance with government code ________. Physical security of network equipment housed at all County occupied sites should remain locked at all times. 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. 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.~~

~~L. Entrances to the data centerre should remain locked at all times. Entry by authorized staff should be by means of a physical key or access card.~~

~~IV.~~ REFERENCES

IV.

~~[Identify Related Policies, Ordinances or Other Codes]~~NIST Publication 800-53 rev. 4, Board Policy A-19 ~~name this here~~General Network Usage Policy, Code of Federal Regulations Title 45 Part 164, IT Data Breach Response Procedure ~~(Jimmy Possible Reference to MS-ISAC for Reporting Protocol)~~

V. RESPONSIBLE DEPARTMENT

Information Technologies

~~V.~~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