COUNTY OF EL DORADO, CALIFORNIA

Subject:	Policy Number:	Page Number:
DATA CENTER AND NETWORK SYSTEMS PHYSICAL SECURITY	A-17	1 of ~~3~~5
	Date Adopted: 06/17/1997	Revised Date: ~~01/04~~09/16/ 2022

I. PURPOSE

The purpose of this policy is to~~:~~

~~A.~~ ~~To~~ establish ~~a policy to set forth~~, in accordance with Code of Federal Regulations, Title 45, Section 164.310 – Physical Safeguards, reasonable and enforceable standards for the physical protection, security, and availability of County data and the facilities in which they are housed, while ensuring that authorized access is allowed.

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~~, and 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~~Data Center. In the event of a ~~data center~~Data Center disaster, a Continuity of Operations Plan (COOP) must be in place to restore critical operations within seven (7) days and files shall be restored to a status reflecting that as of the close of business seven (7) 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

COUNTY OF EL DORADO, CALIFORNIA

Subject:	Policy Number:	Page Number:
DATA CENTER AND NETWORK SYSTEMS PHYSICAL SECURITY	A-17	2 of ~~3~~5
	Date Adopted: 06/17/1997	Revised Date: ~~01/04~~09/16/ 2022

following responsibilities for the physical 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~~;~~.

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

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

3. IT in collaboration with Facilities ~~Maintenance~~Division shall maintain the necessary environmental systems in the ~~data center~~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~~.

4. IT in collaboration with Facilities Division will ensure proper physical security of the ~~data center in accordance with Code of Federal Regulations 45, Section 164.310~~Data Center. 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~~;~~.

1. 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~~Data Center disaster, emergency, or media failure~~;~~.

2. Conduct periodic training and testing on continuity of access to County data to ensure readiness.

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

1. 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~~;~~.

2. 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:

1. Provide physical security for data and computing resources in their custody~~;~~.
2. Identify and classify sensitive data (as specified by the user department~~);~~
3. Identify authorized users of the data (as specified by the user department~~);~~).
4. Identify the potential risk associated with the loss or destruction of data~~;~~.
5. 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.
6. Allow authorized personnel only to the ~~data center~~Data Center for which they are responsible, to perform specific tasks with respect to the installation, maintenance, auditing, and decommissioning of equipment housed there~~;~~.
7. Inform the users of the availability, capabilities, and potential threats or risks of hosted applications~~;~~.

E. Data ~~center~~Center physical security requirements~~:~~.
~~E.~~

1. Entrance doors must remain closed and locked 24/7. Doors may not be left open or unmonitored for any purpose including installing cable or equipment. If an emergency occurs, such as failure of environmental controls, that requires the doors to be left open to support airflow, a designee appointed by the CISO must remain posted within visual range of the entrances to the ~~data center~~Data Center until the doors can be closed.
2. ~~Authorized~~ Individuals granted unescorted ~~access~~Authorized Access to the ~~data center~~Data Center must:
    1. Carry and be prepared to present a valid ~~county~~County identification card or a vendor identification card when in the ~~data center~~Data Center;
    2. Swipe a valid identification card to access the ~~data center~~Data Center. Multiple individuals may not enter a ~~data center~~Data Center using one individual's card; and,
    3. Ensure that Visitors do not handle, damage, or reconfigure existing ~~data center~~Data Center assets in an unauthorized manner.
3. Visitors granted temporary, escorted access to the ~~data center~~Data Center must:

1. Carry and be prepared to present a valid ~~county~~County identification card or a vendor identification card when in the ~~data center~~Data Center;
2. Sign in upon entry and sign out upon exit of the ~~data center~~Data Center, providing the reason for visit. Signing in and signing out is mandatory. Log is stored in the ISO~~.~~; and
3. Always be escorted by an authorized individual within visual range.

4. Access logs must be maintained for a minimum of one (1) year and reviewed quarterly by the ~~Security Office~~ ISO.

~~5. Data center asset physical security~~

5. Maintenance Records. Repairs and modifications related to the physical security of the Data Center facility (e.g., hardware, walls, doors, and locks) must be documented. Such documentation will include date and time of repair or modification, description of the physical component prior to repair or modification, reason(s) for repair or modification, person(s) performing repair or modification, and outcome of repair or modification.

6. Data Center asset physical security:
    1. All assets that have reached the end of their life cycle must be removed from use and be sanitized and removed from the ~~data center~~Data Center.
    2. Only ~~Authorized~~ Individuals with Authorized Access may connect or disconnect any Data Center ~~Asset~~asset.
    3. All installations or removal of Data Center ~~Assets~~assets must be formally documented and reviewed.
    4. Deliveries and/or removal of assets must be indicated on access logs.
    5. Temperature and humidity must be monitored to prevent fluctuations that could adversely affect the ~~data center~~Data Center.
    6. Food, drink, and liquids of any kind are prohibited from the ~~data center~~Data Center.
    7. External electronic equipment (e.g., laptops, vacuums, power tools) and devices (e.g., fans, drills) that are not included on the Data Center Asset Inventory and are temporarily brought into the ~~data center~~Data Center for a specific purpose must be plugged into the nearest standard wall outlet. External electronic equipment or devices may not be plugged into rack outlets.
    8. No personal photography or videography is permitted in the ~~data center~~Data Center without ~~the explicit~~a prior written approval of the ISO.

~~IV. Definitions~~

IV. DEFINITIONS

A. **CISO** - Chief Information Security Officer
B. **ISO** - Information Security Office

C. **Authorized Access** - Access to the Data Center that has been approved by the ISO.

D. **Data Center Asset** - A component located within a data center including, but not limited to, servers, blade systems, network devices, storage devices, racks, and rack power distribution units ("PDUs").

E. **Data Center** - A facility, or portion of a facility, with the primary function to house data processing equipment ~~and~~that features power outage protection~~,~~ and can undergo routine maintenance without affecting operation; however, unplanned maintenance and emergencies may affect operations.

F. **Visitor** - means a person with approved, escorted access to the Data Center.

V. 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

VI. RESPONSIBLE DEPARTMENT

Information Technologies

VII. DATES ISSUED AND REVISED; SUNSET DATES:

Issue Date:	06/17/1997	**Sunset Review Date:**	N/A
Revision Date:	01/09/2018	**Sunset Review Date:**	01/08/2022
Revision Date:	09/13/2022	**Sunset Review Date:**	09/13/2026