



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|-----------------------------|---------------------------------|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 1 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/1507/201722 |

I. PURPOSE

The purpose of this policy is to:

- A. Ensure Information Technologies (IT) strategy ~~is governed by~~ supports the County's Strategic ~~Plan~~ Goals.
 - i. Implement systems that improve system-wide process, data sharing, and departmental collaboration
 - ii. Approach large, complex and/or system-wide matters as one organization – Departments will collaborate on projects and efforts that have cross-departmental impacts
 - iii. Evaluate requests and recommendations based on complete assessment of the best available information, with the goal of reaching well informed decisions
- B. Establish policy and governance procedures for ~~acquisition and life-cycle management~~ the Life Cycle Management of ~~enterprise~~ information systems and technical equipment.

II. BACKGROUND

- I. The application of computer and network-based technologies within the County is a strategic decision. When applied in a cost effective and integrated manner these technologies will provide improved Countywide efficiencies leading to enhanced and expanded public service while controlling ~~the cost of services and service delivery~~. The IT Department is responsible in part to provide that integrating function and to further provide the Board of Supervisors, ~~through the Chief Administrative Officer~~, with an information system strategic plan representing a Countywide approach to applying computer and telecommunications-based solutions.



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|------------------------------------|--|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 2 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/1507/201722 |

III. DEFINITION OF TERMS

- A. **Change Advisory Board (CAB)** - A group of people that support the assessment, prioritization, authorization, and scheduling of changes. While the CAB is not expected to approve changes, their role is pivotal in advising whether a change should be approved. As such, the members of the CAB are expected to be experienced in both business and technology to point out any significant issues that a technical change could result in if not managed properly.
- B. **Change Control Body** - Staff assigned to the Change Advisory Board (CAB) including Infrastructure, Project Management Office (PMO), Security, IT Service Desk, and Applications.
- C. **Breach** - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for unauthorized purpose.
- D. **System Owner** - Person or organization having responsibility for the development functional requirements, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system.
- E. **Data Owner** – Individuals who have direct responsibility for the data that resides and/or is primarily used within their department. The owner is accountable for classifying the data and reviewing the classification.
- F. **Life Cycle Management** - The processes, methods, and procedures associated with the system throughout its life cycle and provides distinct contexts for the interpretation of system security. Life cycle security concepts apply during program management,



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|------------------------------------|--|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 3 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/1507/201722 |

development, engineering, acquisition, manufacturing, fabrication, production, operations, sustainment, training, and retirement.

G. **Risk Analysis** - The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

H. **Intake Process** - Project intake, requirements gathering, approval, and prioritization to balance the IT project portfolio's alignment to four key constraints: stakeholder needs, strategic priorities, standards, and available IT resource capacity for projects.

I. **Protected Data** - Applies to data that must be kept private under State, Federal, County, Tribal, and Local regulations.

i. **PII - Personal Identifiable Information**

ii. **HIPAA - Health Insurance Portability and Accountability Act**

iii. **CJIS - Criminal Justice Information Systems**

iv. **PHI - Protected Health Information**

v. **PCI - Payment Card Information**

III-IV. **POLICY**

- A. The governance of County information systems and technology shall be established in the County Strategic Plan, which is the responsibility of the Board of Supervisors and coordinated by the Chief Administrative Office. The Director of IT is responsible for developing and executing an IT Strategic Plan that is based on, and driven by, the County Strategic Plan. The IT Director is also responsible for implementing a management and operations framework that optimizes the value of IT resources in the planning and execution of IT strategy.



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|-----------------------------|---------------------------------|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 4 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/1507/201722 |

- B. The ~~Acquisition~~ acquisition and renewal of all computer and network technology solutions for the County shall be in support of the IT Strategic Plan, and all such acquisitions and renewals shall be primarily managed by the IT Department. All county Departments shall consult with the IT Department when pursuing technology solutions to ensure acquisitions are technologically sound; will meet business objectives, security and technical requirements, and hardware standards; and are supportive of strategic objectives.
- C. Technical and security requirements shall be designed and implemented to secure County technology platforms and systems. Technical and security requirements shall be required for all technologies within the County environment and must be applied before the platform or system is placed into production.
- D. Equipment standards shall be defined and implemented to ensure computing requirements are met. Departments must select equipment from the standard list or submit a justification for IT Department review. The IT Department will be responsible for ensuring the selected hardware meets standards required by software.
- E. All data within the County's information systems is proprietary; and shall be protected in accordance with State ~~and~~, Federal, County, Tribal, and Local regulations. The department, agency, or entity responsible for creating, entering, updating, or otherwise using a specific portion of data shall be considered the ~~Data Owner-System Owner. The System Owner shall be responsible for addressing all security requirements identified through a risk analysis. The System Owner ensures and maintains compliance with technical and security requirements.~~



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|-----------------------------|---------------------------------|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 5 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/1507/201722 |

C.F. Data Owners are responsible for ensuring the IT Department is aware of special handling requirements for their data including State, Federal, County, Tribal, and Local regulations.

G. The Information Security Office (ISO) shall be responsible for monitoring and measuring compliance and establishing controls to prevent data loss. On a continuous basis, the Information Security Office shall review the established baseline controls for currency and effectiveness. The ISO shall be responsible for the identification of potential data loss and/or other vulnerabilities, the System Owners must ensure timely resolution, as identified by the ISO.

H. All systems must be maintained with supported versions of software, hardware, and operating systems. Any current system's software, operating system, or hardware must also be upgraded if a significant security risk is identified by the ISO. The System Owner and the ISO is responsible for ensuring this requirement is maintained.

IV.V. PROCEDURE

A. The IT Steering Committee and Sub-Committees

- i. Director of IT, in coordination with the Chief Administrative Officer ~~and Director of IT~~ shall establish and maintain a charter for an IT Steering Committee, which is responsible for validating and guiding the execution of the IT Strategic Plan. The committee shall be chaired by the IT Director, and membership shall include all County Department Heads with the understanding that sub-committees ~~may be designated from time to time to work with the IT Director on specific projects/tasks.~~ will be designated for each unit of business defined as General



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|-----------------------------|---------------------------------|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 6 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/1507/201722 |

Government, Law & Justice, Health & Human Services, and Land Use & Development Services.

- ii. The Director of IT shall present a progress report on strategic objectives and updates to the Board at least annually. The IT Strategic Plan shall be no more than three (3) years in scope, due to rapidly changing technology and business requirements.

B. System Planning and Security Requirements Analysis

- i. County departments ~~or agencies shall~~ shall ensure any ~~requirements requests~~ for new technology ~~or renewals~~ are presented to the IT ~~Department Project Management Office (PMO) through the IT intake process~~ prior to beginning the acquisition process and prior to the issuance of Requests ~~For~~ Proposals (RFPs) or bids, if required. The ~~IT Department PMO~~ shall work with the requester to ensure full understanding of business, security, and technical requirements.
- iii. ~~ii.~~ The ~~IT Department PMO~~ shall assist the requester in developing a thorough evaluation process to ensure the chosen technology is cost effective, meets business objectives, security and technical requirements, ~~meets~~ industry and County standards, and is in concert with County strategic objectives. The PMO will maintain a project portfolio tracking all requests for projects. The PMO will work with sub-committees to discuss collaboration projects, if a solution is already in place, and aligned County Strategic Goals. The PMO will ensure resource allocations are understood for both business and technology support



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|------------------------------------|--|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 7 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/1507/201722 |

throughout the System Life Cycle to ensure sustainable systems are selected and maintained accordingly.

- iii. The ISO and Infrastructure division shall develop technical and security requirements in the form of procedures, process, guidelines, comprehensive questions, and configurations to ensure consistent compliance with the County information security policies and standards.
- iv. The ISO shall work with System Owners to perform risk analysis for each new application, application renewal, existing applications, or major system change. The results of this risk analysis must incorporate safeguarding information, data retention, policy compliance, data governance, disaster recovery, and business continuity, regarding security threats and vulnerabilities that may exist and a recommended plan of action. Depending on the classification of data (e.g., PII, HIPAA, CJIS, PHI, PCI, etc.), specific security requirements and security controls must be incorporated within the application selection process, discovery, design, analysis, development, testing, pre-production implementation, production implementation, and continued maintenance/support of the system.
- v. The desktop and infrastructure divisions shall develop platform and equipment standards with recommended use and life expectancy of equipment.
- vi. The desktop and infrastructure divisions will perform a review for new hardware and platforms. If hardware requests are not defined on the standard equipment list the department must submit a justification for technical review and



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|-----------------------------|---|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 8 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/ 1507 /20 17 22 |

approval. All purchases must follow the County Procurement Policy (Policy C-17).

C. System Testing

- i. County departments are responsible for ensuring adequate testing is completed and the system is accepted by system owners prior to use. Any substantial changes to application functionality must be formally documented and the documentation made available to the ISO for later verification of required security functionality.
- ii. The PMO assists the County departments by offering Test Plan templates.

D. System Implementation and Maintenance

- i. The IT Department shall establish a formalized Change Advisory Board (CAB). All promotions to the production environment shall be approved and coordinated with the Change Control Body.
- ii. The IT Department is responsible for ensuring technology and processes are in place to provide the requisite protection levels as specified by the ~~Data Owners.~~ system Owners according to the data classification, data loss protection requirement, data compliance, data retention, and disaster recovery.
- ~~iv-iii.~~ In the event of a breach, unexpected loss or corruption of protected data, the Risk Management Division of the Human Resources Department shall ensure any required reporting, notification, information, inter departmental collaboration, contacts (County, vendor, and contractors involved), and



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|-----------------------------|--|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 9 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/ 1507 /20 1722 |

mitigation actions are taken. The ~~IT Department~~Information Security Office (ISO) and System Owners shall work with County Risk Management in such cases, and is responsible for providing ~~any technical~~ information ~~or~~and support necessary to meet notification requirements.

E. System Decommissioning

- i. Prior to decommissioning, the County Department with the Security Office, shall formalize plans describing the processes to properly remove and protect sensitive data from the systems to be decommissioned.
- ii. System Owners will certify and validate decommissioned systems, property, equipment, and data meets Federal, State, County, Tribal, and Local decommissioning compliance.

~~V~~.VI. REFERENCES

~~_____~~ N/A

~~_____~~ C-17 Procurement Policy

~~_____~~ Equipment and License Standards: A-13 Equipment Standards.xlsx (sharepoint.com)

~~VI~~.VII. RESPONSIBLE DEPARTMENT

Information Technologies/~~Chief Administrative Office~~



COUNTY OF EL DORADO, CALIFORNIA

BOARD OF SUPERVISORS POLICY

| | | |
|--|-----------------------------|--|
| Subject: COMPUTER AND NETWORK-BASED INFORMATION SYSTEMS POLICY | Policy Number: A-13 | Page Number: 10 of 10 |
| | Date Adopted: 04/06/1993 | Revised Date: 11/ 1507 /20 17 <u>22</u> |

VII.VIII. DATES ISSUED AND REVISED; SUNSET DATES:

| | | | |
|-----------------------|------------------------------------|----------------------------|------------------------------------|
| Issue Date: | 04/06/1993 | Sunset Review Date: | NA |
| Revision Date: | 11/07/2017 | Sunset Review Date: | 11/06/2021 |
| Revision Date: | 10/25 <u>11/15/2022</u> | Sunset Review Date: | 10/24 <u>11/14/2026</u> |