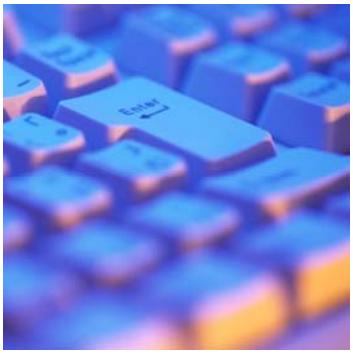
Updated 3-16-2009

El Dorado County

Computer and Network Resource Usage Policies and Standards Guide

Departmental IT Staff



INTRODUCTION

This Computer and Network Resource Usage Policies and Standards Guide, for County Departmental IT Staff, has been created to assist El Dorado County employees in understanding their responsibilities when using or deploying County computers, printers, peripherals, software, and network resources. The Guide is intended to comply with Board Policy A-19.

Due to new regulatory requirements, this document has increased emphasis on security requirements. These requirements affect many departments using various applications or working with documents in protected classes, such as the Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII), and Protected Health Information (PHI).

The following pages delve deeper into these new security requirements and their impact on you, and your respective departments.

Page 18, “Departmental Information Technology County User Agreement” must be signed by all County departmental IT staff indicating they have read and understand this entire document. The original signed document must be returned to the Information Technologies Department. Departments should retain a copy of this document for their records.

As this document may change, all IT departmental employees must re-sign the User Agreement once a year. It is suggested that this be done at the time of their annual evaluation.

TABLE OF CONTENTS

DEPARTMENTAL INFORMATION TECHNOLOGY STANDARDS AND GUIDELINES

Department heads are responsible for ensuring all IT Administrators under their control have fully read and understand every aspect of this Computer and Network Resource Usage Policies and Standards Guide.

Department heads are also responsible for providing the appropriate computing tools for their County users to maximize the return on the technology investment and to provide them with adequate tools to complete their assigned tasks.

This document provides descriptions of "standards" for personal computer systems, servers and related systems, peripherals and software to be used throughout El Dorado County (County). Additionally, this document will be used to establish common security and computer usage guidelines for all County departments. The objective of these recommendations is to standardize computer configurations and software in El Dorado County. The goal is to recommend the best possible systems that meet County user requirements and at the same time maintain a reasonable total cost of ownership.

Together with these recommended systems are specified a standard set of productivity and communication client software tools. By implementing hardware and software standards, the County will enable its personnel to communicate and collaborate, and reduce support and training costs. It is recommended that no software be more than 2 versions behind the current offering from the applicable vendor.

The implementation of Countywide technology standards ensures that the County will position itself to take advantage of the many benefits and protections that come with a standardization plan. Standards will also minimize total information technology costs.

Deviations from these standards may occur based on specific departmental technical needs. Deviations must be reviewed and approved by the Director of Information Technologies or designee. IT decisions may be appealed to the IT Steering Committee.

The benefits reflected in a Countywide standards implementation are:

- Interchangeable data and formats utilized by all departments.
- Manageable and cost effective Countywide upgrades to operating systems, office applications, communications/emulation software, security/virus protection software, etc.
- Economies of scale utilized in purchasing, deployment, and support of the Countywide information technology environment.
- Standardized training and general understanding of the operational aspects of standardized software and hardware.
- Countywide assurance of connectivity of workgroup environments such as electronic communication, calendar, e-meetings, etc.
- Countywide quality assurance of technology.

Information Technologies (I.T.) and El Dorado County department IT staff together will negotiate with vendors for the best price/performance value for the recommended hardware and software in this document. Support and training will be available in accordance with these recommended standards. To keep pace with technology, the hardware, software, software version levels, and specifications presented in this document will be reviewed and updated when appropriate or required.

1.1 Hardware and Software Standards and Guidelines

1.1.1 Operating Systems (OS)

Desktop Systems:
Microsoft Windows XP Professional is the County's desktop operating system standard. This standard will optimize installation and support while maximizing flexibility and the ability to ensure compatibility of additional layers of connectivity and application software.

Discussions and evaluation regarding migration from Windows XP to later releases of Windows are continuing at this time.

PC Server Systems or Network Operating Systems (NOS):
Microsoft Windows is the County's standard server operating system, using Active Directory Services (ADS).

1.1.2 Desktop Computers (Office Personal Computers) and Monitors

Computers manufactured by Dell Computer are the County's standard hardware platform. If assistance is needed in determining the hardware that is required by your software needs, please contact I. T.

During the installation of office suite applications, the installer should reference the intranet IT standards page for proper machine, and application naming conventions. These conventions would apply to first time setup of the applications.

Monitor configurations vary with the intended use. Non-standard monitors require approval of the department head and CAO's office. Specifications for standard configurations can be found at the website below

Specifications for Desktop computers and monitors can be found on the I.T. intranet website:

http://edcnet/IT/PUBLIC/index.html

1.1.3 PC Laptop (Notebook) Computers

The current County standard for laptop (notebook) computers is Dell. All mobile computing equipment should be equipped with BIOS/Hard Drive password protection. Devices containing confidential or regulatory protected data shall use Pointsec hard drive and portable media encryption to provide maximum protection against un-authorized access to data contained on the device. All laptops shall be equipped with Computrace Plus to aid in the recovery of stolen or lost laptops.

Specifications for laptop computers can be found on the I.T. intranet website:

http://edcnet/IT/PUBLIC/index.html

1.1.4 Cellular Personal Digital Assistants (CPDA's) Specifications

While there are numerous vendors with many compatible products the specifications below represent the standard:

Physical Memory	64 MB minimum
Operating System	Windows 5.0 or greater/Blackberry Operating System 4.0 or greater
Connectivity Software	IBM Lotus Notes Traveler or Blackberry Enterprise Server

Existing Palm operating system based devices will be supported through their end of life and then will no longer be supported.

If assistance is needed in determining the appropriate CPDA that is required by your software needs, please contact I. T.

1.1.5 Printers

Standard County printers include Hewlett Packard, Dell and Xerox. The use of desktop printers is limited to staff printing confidential information, primarily personnel related. All departments should strategically place workgroup or enterprise printers as applicable to serve your printing needs. Supported printers shall include ink jet (limited use and deployment), laser and dry ink technology based devices. Devices may include single purpose printers or multifunction devices.

I.T. assists departments in determining their exact needs and must be notified prior to connecting network printers to the WAN. Printer standards may be found on the I.T. intranet website:

http://edcnet/IT/PUBLIC/index.html

The County has a maintenance contract with an outside vendor. Problems with printers should be reported to I.T. on a trouble ticket and I.T. will coordinate the maintenance with the vendor.

1.1.6 Network Server Specifications

Servers need higher CPU and I/O performance and reliability than that of their associated client desktops. The server must incorporate features that allow it to support the environment for its intended use. It may be used as a database server, an application server, or as a file and print server. Uses may be specific for a departmental application, or may be for general departmental or Countywide use**.**

Standard server configurations must include the following depending on their use:

- Windows 2003 Server. Further discussion and evaluation is required before migration to Windows Server 2008 can be recommended.

- Microsoft IIS version 6 is the current County web server standard. Testing and certification of IIS version 7 is underway with implementation started after the new system has been tested and approved by the I.T. department.

- Minimum 3 years on parts and labor, onsite, same business day, 3 years of 24X7 hour response on mission-critical servers.

1.1.6.1 General Server Configuration Specifications

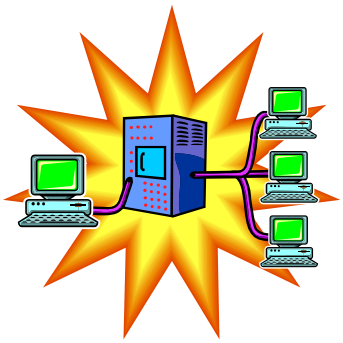
Server specifications can vary greatly depending upon the application being run. Departments should always consult I.T. for assistance with server specifications. General specifications can be found on the I.T. intranet website:

http://edcnet/IT/PUBLIC/index.html

1.1.7 Disposal of Surplus Computing Equipment

Prior to being surplused computers must have data permanently and thoroughly destroyed. Methods similar to those of the Department of Defense formatting process should be performed on hard drives or other permanent data storage devices. This process typically consists of seven (7) passes alternating writes with 0 and 1 bits. Hard Drives and all forms of media may also be shredded by a certified destruction firm. Contact the I.T. department for further information.

Normal surplus procedures defined by Procurement & Contracts must be used to dispose of surplus County property.



1.2 Network Infrastructure, Server And Network Administration Standards And Guidelines

County offices and computers are connected to networked resources through a Wide Area Network (WAN). The I.T. department administers the wide area network (WAN) and the vast majority of networked resources attached to the County's WAN. Effective implementation of these standards and guidelines will minimize unauthorized access to County proprietary information and technology and ensure reliable delivery of networked resources. Many factors must be considered prior to the introduction of any application, network device or server to the WAN.

1.2.1 Ownership and Responsibilities

The majority of all file and print, application, electronic communication, Internet and intranet web, enterprise servers deployed in the County are administered by I.T.

The County's business information, telephone, network, computer and software resources, peripherals and supplies are County property and are intended to be used to conduct County business.

All data created or received on the County's computer systems remains the property of El Dorado County. There is no reasonable expectation of privacy regarding the confidentiality of information stored on any computer, CPDA, terminal or network device belonging to El Dorado County, whether related to County business or to personal use.

It is the responsibility of the departmental IT staff to safeguard confidential information from unauthorized disclosure or use. They must take all reasonable precautions to ensure privacy is maintained under the law, when exposed to confidential information, including but

not limited to voice, electronic (disk file, diskette, CD ROM, DVD, magnetic tape, electronic communication, etc.), paper, photographs, and microfiche.

Access to another County User's data must not be granted without written or electronic communication authorization from the appropriate department head or designee. All electronically stored data remains the property of El Dorado County; intentional destruction of this property is prohibited.

The I. T. department must authorize the connection of devices other than County owned desktop or laptop computers prior to insertion into the WAN or the joining of any server to the Microsoft Active Directory environment. Configuration changes for production servers must follow appropriate change management procedures as established by the I. T. department.

1.2.2 General Guidelines

- Services and applications that will that are no longer in use must be disabled.
- Access to services should be logged and/or protected through access-control methods.
- All servers and computing equipment must have the latest approved patches, service packs and antivirus software installed on the system prior to placing the equipment into production.
- Departmental IT server administration staff should always use standard security principles of least-required-access to perform a function.
- Servers should be physically located in a secure and access-controlled environment.
- Servers are specifically prohibited from operating from unsecured or uncontrolled cubicle areas.
- I.T. server administrators maintain the root of the ADS environment.
- Departmental network administrators may be delegated administrative access and rights to their departmental domains. I.T. shall establish the level of administrative access granted to departmental IT staff based on need. Administrators are strictly forbidden from browsing or otherwise accessing the files of County users without authorization from the Human Resources department and/or the respective department head.

1.2.3 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved **at a minimum**, as follows:

- All security related logs must be kept online for a minimum of 1 week.
- Daily incremental tape backups of logs must be retained for at least 1 month.
- Weekly full tape backups of logs must be retained for at least 1 month.

Security-related events will be reported to I. T. department, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks.
- Evidence of unauthorized access to privileged accounts.
- Anomalous occurrences that are not related to specific applications on the host.

1.2.4 Server Account Deletions

Upon notification by Human Resource (HR) or a department head (or designee) that a County user is confirmed to have permanently left County service, the accounts administered by I.T. (network and email) will be frozen or deleted. The data files will be moved to "obsolete status". Files placed in "obsolete status" are retained for 60 days and then deleted. Departments may request an extension to file retention after approval from HR. The request should be sent from HR to the I.T. department prior to the 60 day standard. Upon acceptance, I.T. will retain the files an additional 30 days.

1.2.5 Compliance

Audits of Network Infrastructure, Server and Network Administration Standards and Guidelines will be performed on a regular basis by authorized I.T. personnel. Out of compliance findings will be reported to the I.T. Director and to the affected department head.

1.2.6 Forensics

All requests for employee email and/or Internet monitoring will be made according to these procedures:

(1) Department head or authorized management shall request employee email or Internet monitoring via memo or email to HR;

(2) Requests approved by HR shall be forwarded to the Director / Assistant Director of I.T.;

(3) Director / Assistant Director of I.T. shall forward the request for monitoring to the Manager – Technical Support/Security Officer, who, with a designated network security analyst, will initiate the authorized monitoring, compile and analyze all findings;

(4) The Manager – Technical Support/Security Officer shall report the results to HR for appropriate action in conjunction with the requesting department.

I.T. shall remain neutral regarding County employee's use of email and Internet services. Monitoring of specific activities shall be strictly limited to authorized departmental requests. I.T. staff shall make no independent queries into employee email or internet usage; however, secondary inappropriate internet use discovered during the course of authorized monitoring shall be reported to the Director / Assistant Director of I.T. and HR for appropriate action.

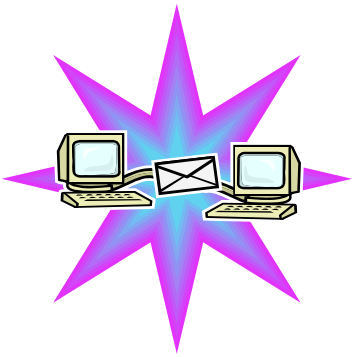
Due to the confidential nature of information contained on the appliance the device console shall remain locked at all times except during authorized use. County computers used to

access the appliance via the County network shall remain locked whenever the network security administrator(s) are away from their computers. Network access to the appliance and administrator rights for the installation of remote access software used to access the appliance shall be restricted to a designated network security analyst's computers Investigatory work performed on network access computers shall be performed in a secure manner, out of public view, and from a visually secure location.

Failure on the part of the administrators to follow and adhere to these policies and procedures or to misuse their administrative access for unauthorized logging and/or monitoring internet usage could result in disciplinary action up to and including termination of employment.

1.3 Network Addressing Standards

1.3.1 Background



TCP/IP will be the County standard network communication protocol. All devices in the County Intranet shall be addressed in accordance with best practices specified in Request for Comment 1918 (RFC1918, address allocation for private networks).

Each location will have its own subnet. In larger County locations and facilities, addressing might also follow wiring and switching topology documented in the County network diagram.

All addressing will be established and controlled by I.T. staff to ensure Countywide security and adherence to address inventory, to avoid address conflicts, and prevent potential destruction of the respective network. Within each subnet, conventions will be established assigning static ranges of addresses to printers, servers, Dynamic Host Configuration Protocol (DHCP), secure terminals, switches, hubs, etc.

All computers, laptops, servers, printers or other devices that will be connected to the County's Wide Area Network (WAN) must use TCP/IP addresses supplied by the I. T. department via DHCP or static addresses. The I. T. department administers all devices serving TCP/IP addresses on the County WAN. All Domain Name System (DNS) services, which is a hierarchical naming system for computers, services, or any resource participating on the network, will be provided and managed by I.T.

Computers accessing outside services via modems or wireless connections to a foreign network may not be simultaneously attached to the County's Wide Area Network. To provide access to the County's Wide Area Network, Virtual Private Network (VPN) connections to the County network through the public Internet can be granted by contacting the I.T.

I.T. must be notified prior to installing any network-attached device on the El Dorado Countywide Area Network, especially when new PCs or servers are removed from any domain or tree. This notification requirement will allow I. T. to prepare properly for the introduction of new equipment to the respective environment and plan to respond rapidly to potential problems within the network caused by the introduction of new or moved network attached devices. All networked devices shall have a County issued Gold Asset tag affixed to them. This tag and its respective number are used in conjunction with departmental initials to identify the device on the network.

1.3.2 Network Naming Conventions

The following server and PC "naming convention standards" shall be used to ensure network stability, increased support capabilities, and enhanced diagnostic abilities within the IT Technical and Network support groups:

- Server authentication shall use first name, last name.
  Computer names shall be based on the departmental initials and the devices asset tag.

- Servers shall be named using the department initials followed by descriptor initials denoting the devices level of service. For example a file and print server in the I.T. department would receive the network name ITFS1, ITFS2 etc., dependent upon the number of files and printer servers. Application servers shall receive names based on departmental initials followed by AS1, AS2, etc.

Contact the I.T. department with any questions regarding naming conventions.

1.3.3 Machine Identification, Workgroup Names

Computer names shall be based on departmental initials and asset tag number. Contact the I.T. department with any questions regarding desktop or laptop naming conventions.

1.4 Applications Standards and Guidelines

1.4.1 Applications

Desktop: Microsoft Office Professional 2003 Suite is the County's standard office productivity tool. This "suite" includes Word, Excel, PowerPoint, Publisher, and Access.

Mainframe Access: TN3270+, produced by SDI, is the County's standard emulation software.

Anti-Virus: The County's anti-virus, firewall and malware protection software standard is McAfee for desktop computers, laptops, wireless and standard personal digital assistants and servers. Anti-virus software will be continuously updated to ensure that we have the most up-to-date protection available.

Email/Calendaring: Lotus Notes **8** is the County's standard email, instant messaging and calendaring application.

Web Browser: Microsoft Internet Explorer 7 is the County's current standard Internet Browser.

Imaging: The County's standard imaging system is EMC's Application Extender.

Voice Recognition: Dragon Naturally Speaking is the County's standard voice recognition software.

1.4.2 Application Development

As the number of and demand for applications, web and otherwise, continue to rise at the County, the ability to maintain a stable production environment becomes increasingly difficult. In order for I.T. to be able to meet the business requirements of the County, as well as to minimize the likelihood and impact of errors in the production environment, a standard set of application development tools and guidelines is needed.

This section discusses those tools and guidelines specific to multiple tier application development, which includes:

- Web Apps multi-tier applications delivering a browser based User Interface which extends beyond the user presentation and navigation layer.

- Windows Apps: multi-tier applications delivering MS Windows based User Interface.

As the County's infrastructure changes so will these tools and guidelines. Questions concerning this information should be directed to I.T.

1.4.2.1 Application Development Planning and Review

All plans and proposals by County departments for application development must be submitted to I.T. for formal review prior to the initiation of any development related activities.

I.T. will complete the review in a timely manner, within a time frame commensurate with the size and scope of the request. Within 3 days of receipt of the request I.T. will notify the requestor of the estimated date of completion of the review. Unanticipated delays in the review will be promptly reported to the requestor.

As defined in Board of Supervisors Policy A-10, Information Technologies Steering Committee and Acquisition Procedures, I.T. shall refer all requests involving enterprise (multi-department) applications and/or new systems development projects exceeding $10,000 to the ITSC.

Departments who are currently utilizing or may be looking at procuring applications developed outside the County should also review and adhere to Board of Supervisors Policy A-10.

1.4.2.2 Role of Departments in Application Development

Some County departments have staff whose primary role within their department is to provide IT support and services to their organization. They possess IT skills and knowledge that exceed those of the average user base. The model that would be most beneficial for the County as a whole would be one that establishes this group as a partner with I.T. in the development process.

The role of these development partners would be to supplement IT development in order to meet the growing demand for applications at El Dorado County. If IT resources are not available to meet the required schedule for development of a new application, then the development could be performed by a department partner instead.

Departmental development of applications must be conducted in a true partnering relationship with IT. This would entail IT involvement from the beginning of the development cycle in the form of preliminary and initial consulting. IT will fill an advisory

and facilitating role throughout the development process. The application should be submitted for review and final approval by IT before it is moved to a production environment.

1.4.3 Data Environment

In the County's current environment the primary data source for non-legacy systems has been Microsoft Access. Access is a single-user, desktop based office productivity tool. It is not designed, nor is it meant to serve as the data store for enterprise applications—be they web-based or otherwise.

In order to position I.T. to be able to deliver high performance, highly scalable solutions, MS SQL (structured query language) has been adopted as the County's enterprise relational database.

At this writing policies and guidelines are being developed. Those planning to develop with MS SQL should contact County I.T. for the latest policies and guidelines governing its use.

1.4.3.1 Access to Legacy Systems/Data

Access to legacy systems/data is an issue of considerable magnitude related to application development, considering the fact that the majority of the County's business data is stored in legacy systems (i.e., FAMIS, ADPICS, HR/PR, Property, LMIS). This makes the use of such data in applications a tricky and indirect process.

The legacy system platform consists of one IBM z9 (Business Class) server, with attached IBM storage, running z/OS, CICS/TS, COBOL, M204, DB2, VSAM, and other operating system software necessary to support the platform.

As a result, development of any application accessing or updating legacy systems/data is restricted to County I.T., unless the department has historically been responsible for legacy systems/data support.

1.4.4 Tool Set

The selection of a standard tool set for use in application development must be compatible with pre defined standards which already exist at lower levels in County IT architecture, such as desktop and server operating system, web server platforms and networking infrastructure. Applications, whether they are web-based or otherwise, run at the highest layer of the OSI model and thus directly depend upon the technologies utilized at the lower layers to function and perform adequately.

Since the current County standards for the processes running at these sub layers are primarily Microsoft products, I.T. has selected the MS Visual Studio toolset as the County's standard development environment (IDE).

In addition, the Adobe suite of products, primarily Dreamweaver and Acrobat Pro, are the County's standard web presentation and forms development tools.

Applications developed using tools or technologies different from those contained in this tool set, which have not received prior approval, may not be supported, maintained or enhanced by I.T.

1.4.4.1 Reporting Tools

Crystal and SQL Reporting Services (SRS) are the County's standard reporting tools. These toolsets will be periodically re-evaluated as emerging technologies mature.

1.4.5 Web Presentation and Accessibility Standards

The Board of Supervisors has expressed a strong desire for the County to maintain a single website.

Board policy A 22, County Website Policy, states in part:

> *"It is very important for the County to maintain one identity on the Internet, so that citizens know that the information they are receiving is official information from El Dorado County. Web pages created by County departments should comply with graphical and navigational standards to maintain a consistent look and feel to the entirety of the County's web presence".*

El Dorado County has a complex environment for web management. The complexity derives from a variety of services, a multitude of audience types and distributed web management responsibility.

This complexity presents a number of challenges for site users and site managers. Two primary challenges are:

- Determining the level of consistency required across the County's website for usability and accessibility.
- Balancing the need for line of business, campaign, and/or department branding needs with County branding needs.

The County's set of presentation standards will address the above challenges.

Due to the pending implementation of a County content management system (CMS) and the redesign of the County's website, the current web presentation standards are being revised.

Until the new presentation standards are developed, staff currently responsible for departmental website support should contact County I.T. for the latest standards and guidelines.

Departmental Information Technology County User Agreement (All County IT Positions)

El Dorado County
Information Technologies Security & Standards Policy
Departmental IT Staff Acknowledgement

I have read and fully understand the El Dorado County "Computer and Network Resource Usage Policies and Standards Guide". I understand as a departmental Information Technology staff member, contractor, sub-contractor or governmental affiliate who may use the El Dorado County's networked resources that I must fully comply with the terms and conditions of this policy. I also agree to remain informed of and comply with future revisions to this policy.

Departmental Information Technology Administrators of the County's network and attached devices may have access to and responsibility for sensitive resources that are connected within the County network. To assure security throughout the entire County network, it is critical that all administrators actively support and fully comply with the measures described in the El Dorado County "Computer and Network Resource Usage Policies and Standards Guide". Failure to comply can place the entire County network at serious risk; and administrators who fail to comply will be subject to disciplinary action. Department heads are responsible for ensuring all Administrators under their control have fully read and understand every aspect of this Standards and Policies document.

Department heads, and all County IT staff shall at all times act in accordance with all applicable laws and County policies, rules or procedures. No County user shall use the Information Technology systems in an improper, inappropriate or unauthorized manner as defined in the "Computer and Network Resource Usage Policies and Standards Guide" document and/or revisions thereof.

Information Technology County User:

Name: _____

Title: _____

Signature: _____

Date: _____

This original signed and executed document shall be returned to the Information Technologies department. This document will be signed annually and a copy shall be retained in department, district or agency files.