El Dorado County

Computer and Network Resource Usage Policies and Standards Guide

General Use

Approved by the Board of Supervisors August 18, 2009

INTRODUCTION

This Computer and Network Resource Usage Policies and Standards Guide has been created to assist El Dorado County employees in understanding their responsibilities when using County computer workstations, printers, peripherals, software, and network resources. The Guide is intended to comply with Board Policy A-19 and applies to all County employees.

There are a number of changes to this latest revision of the Computer and Network Usage Policies and Standards Guide. The majority of these changes are driven by new regulations from various government agencies that necessitate an increased focus on security and the protection against loss or theft of data in protected classes. These classes include the Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII) and Protected Health Information (PHI), Sarbanes-Oxley, etc.)

Page 12, "El Dorado County Computer and Network Resource Usage Policies Agreement" must be signed by all County employees indicating they have read and understood the General Usage Policies, "1.1 – Background" through "1.14 – Remote Access Policies".

It is mandatory that the employee sign the Agreement on an annual basis. It is suggested that the employee re-sign the Agreement at the time of their annual evaluation.

SECTION 1
TABLE OF CONTENTS

1 GENERAL USAGE POLICIES 1

1.1 Background 1

1.2 Purpose 1

1.3 General Use and Ownership 2

1.4 Use of Personally Owned Software and Equipment 3

1.5 Compliance with Software Copyright Laws 3

1.6 Disposal of Copyrighted Software Material 3

1.7 Use of Computer Resources 3

1.8 Use of Electronic Communication 4

1.8.1 Definitions 4
1.8.2 Personal Use 5
1.8.3 State and Federal Laws 5
1.8.4 Restrictions 6
1.8.5 False Identity 6
1.8.6 Representation 6
1.8.7 Network Capacity 6
1.8.8 Possession 6

1.9 Use of the Internet 7

1.10 Computer User ID's and Password 7

1.11 Computer Viruses 8

1.12 Removable Data Storage Devices 8

1.13 Portable Computing Devices (WPDA, PDA, Laptops, Tablets) 9

1.14 Remote Access 10

2 COUNTY USER AGREEMENT 12

3 GENERAL USAGE STANDARDS AND GUIDELINES 13

3.1 Electronic Communication 13

3.1.1 Security and Confidentiality 13
3.1.2 Anti-Spam Measures 13
3.1.3 HIPPA and Compliance with Electronic Communication Privacy Act 14
3.1.4 E-mail Retention 14

3.1.5 Managing E-mail 14
3.1.6 Electronic Communications – Instant Messaging 16

3.2 Passwords 16

3.2.1 Password Construction Guidelines 16
3.2.2 Password Protection Standards 17
3.2.3 Application Development Password Standards 18
3.2.4 Pass Phrases 18
3.2.5 Use of Passwords and Pass Phrases for Remote Access Users 19

3.3 Server Storage Utilization 19

3.3.1 File Storage Options 19
3.3.2 Server File Storage 19

GENERAL USAGE POLICIES

1.1 Background

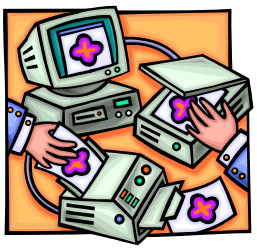
El Dorado County has an extensive communication infrastructure with network and computing resources for use by County employees, contractors, vendors, quasi-governmental employees (fire departments, community services districts, etc.) and temporary workers, hereafter referred to as "County User". In addition, the County provides a large and continuously growing number of computer workstations, printers, peripherals, software, training, and supplies to all County sites. These items are provided by El Dorado County to allow County Users to perform tasks efficiently to meet the goals established by the El Dorado County Board of Supervisors.

While most are familiar with the term "computer", it is only one of the resources that are collectively known as network resources. Network resources consist of computers and their associated peripherals. These network resources, applications, and data provide the means to deliver services to El Dorado County residents.

While much of the data used by El Dorado County is "public" information, with legislative changes (HIPAA, PII, PHI, Sarbanes-Oxley, etc.) there is a need to safeguard the data the County uses and to maintain the security and privacy of that data. Automatic and procedural security controls are in place to prevent or reduce unauthorized access to these resources. The primary responsibility for maintaining the integrity, security, and privacy of this information and its resources lies with the County User.

All computer systems furnished by the County, including but not limited to computer equipment, software, operating systems, storage media, and network accounts providing electronic communication, file storage, Internet access ("www" browsing, use groups, etc.) and FTP (File Transfer Protocol), are the property of El Dorado County. These systems are to be used for business purposes in serving the interests of the County in the course of normal operations. Improper use of any of these resources can result in lost or degraded services to some or all County Users. Violation of local, State and Federal laws, rules and policies may call for prosecution under the law, including fines and imprisonment and disciplinary action.

County Users are responsible for reading, understanding, and following the appropriate use of County equipment and the release of County data. This document summarizes policies and offers standards and guidelines regarding the integrity, security, and privacy of County data, network resources and computers. County Users should contact their supervisors for any necessary clarification.



1.2 Purpose

The purpose of these policies is to define the acceptable use of computer equipment and networked resources throughout El Dorado County. These policies are in place to protect the County User and El Dorado County. Inappropriate use exposes El Dorado County to risks including but not limited to virus attacks, compromising network systems and services, and potential civil or criminal litigation. These

policies apply to all computer equipment that is used by County Users or any device connected to the El Dorado County network.

Deviations from these policies may occur based on specific departmental technical needs. Deviations must be reviewed and approved by the Director, Information Technologies (I.T.) or designee. I.T. decisions may be appealed to the IT Steering Committee.

1.3 General Use and Ownership

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. They do not belong to individuals and are used by County Users for the purpose of completing the work required for their position while employed or contracted by the County.

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, terminal or network device belonging to El Dorado County, whether related to County business or to personal use.

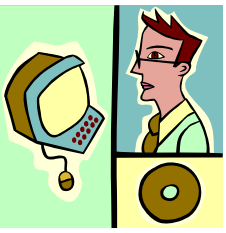
It is the responsibility of the County User to safeguard confidential information from unauthorized disclosure or use. County Users shall not seek to use personal or confidential information for their own use or personal gain. County Users must take all reasonable precautions to ensure privacy is maintained under the law while handling information in any form, including but not limited to voice, electronic (disk file, diskette, CD ROM, DVD, magnetic tape, electronic communication, etc.), paper, photograph, and microfiche information.

New regulatory requirements dictate computers processing protected classes of information (HIPAA, PII, PHI Sarbanes-Oxley, etc.) have their hard drives encrypted. Additionally portable media devices used to store protected classes of information must also be encrypted (USB storage devices, etc.). Portable computers (laptops, notebooks, cellular based personal digital assistants (CPDA)) must be encrypted, contain software designed to recover lost or stolen devices, and have the ability to be remotely incapacitated and able to destroy all data on the device).

Access to another County User's data will 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.

County Users are responsible for exercising good judgment regarding the reasonableness of personal use on personal time. County Users may engage in reasonable incidental personal use of the County's computer systems, to the extent permitted by the County User's department head, as long as such use does not degrade overall system performance (such as streaming media, i.e. music or video files), detract from a County User's productivity, duties, service to the public or to the County, violate any law, or any County policy, procedure, or regulation or tarnish the image of the County or contribute to the disrepute of the County.

For security and network maintenance purposes, I.T. staff members may monitor equipment, systems and network traffic at any time. This monitoring shall be done under the auspices of this policy, which is incorporated into Board Policy A-19.



1.4 Use of Personally Owned Software and Equipment

Personally owned software may not be installed on County computers, nor shall personally owned computer hardware or peripheral equipment be connected to County computers or attached to the County network.

1.5 Compliance with Software Copyright Laws

A copyright violation exposes the County to substantial risk of legal liability. County Users may not:

- Install any software without having proof of licensing; or
- Install software licensed for one workstation on multiple machines; or
- Install or distribute "pirated" or other software products that are not appropriately licensed for use by El Dorado County; or
- Install personal or non-County standard software or peripherals.

County Users may not make unauthorized copies of copyrighted material including, but not limited to, photographs from magazines, books or other copyrighted sources, copyrighted music, or any copyrighted software for which the County or the County User does not have a valid license.

1.6 Disposal of Copyrighted Software Material

All copyrighted material must be disposed of in such a way as to render it useless and to minimize the potential liability to the County. The media on which the copyrighted material was obtained must be physically destroyed (for example, CDs, DVDs or floppy disks, will be broken in half or shredded) and any license keys or any other information that is required in order to use the software legally must be destroyed.

1.7 Use of Computer Resources

County computer resources are used by hundreds of County Users. To ensure that these resources are available and working properly, personal use of these resources must not negatively impact others.

No County User may attempt to access computer systems, or their resources, unless proper authorization has been granted by the department head. Any attempt to maliciously alter, erase, damage, destroy or make otherwise unusable or inaccessible any data, software, computer, or network system may constitute a felony and may result in any combination of

disciplinary action and/or prosecution and fines, including litigation costs and payment of damages under applicable Local, State, and Federal statutes.

No County User shall willfully or through negligence introduce a malicious program into the network, any server or computer, (e.g. virus, worm, Trojan horse, electronic communication bomb etc.), nor shall any County User use port scanners or other intrusive software intended to undermine the stability and integrity of the County network and attached resources.

No County User shall use a County computing resource to engage in procuring, viewing or transmitting material that is pornographic in nature or is in violation of sexual harassment or hostile workplace guidelines. In general, any material that may be considered objectionable or may tend to bring the County into disrepute may not be sent via the County's computer systems.

El Dorado County has a significant investment in network server hardware and associated data storage capacity. Please see General Usage Standards and Guidelines – 3.3 Server Storage Utilization for options and recommendations for the file storage options, directory structure and back-ups to maximize available server storage space.

1.8 Use of Electronic Communication

The need to manage electronic communication systems properly can be viewed the same as other records keeping systems; namely, to ensure compliance with laws concerning the creation, retention, or access to such electronic communication documents and to manage resources storing such electronic communication documents.

El Dorado County government agencies that use electronic communications have an obligation to make County Users aware that electronic communication messages, like paper records, must be retained and destroyed according to established records management procedures. They should deploy, or modify, electronic communication systems to facilitate electronic records management. Specific procedures and processes will vary according to departmental needs and the particular requirements placed on them via specific governmental agency rules or applicable law.

Please see General Usage Standards and Guidelines – 3.1 Electronic Communication for detail standards in support of these policies.

1.8.1 Definitions

Electronic communication ***systems*** transport messages (store and deliver) from one computer user to another. Electronic communication systems range in scope and size:

- From a local area network electronic communication system that delivers messages within an agency or office.
- To a wide area network electronic communication system that carries messages to a variety of physical locations.
- To Internet electronic communication that allows users to send and receive messages from around the world.

- All County e-mail shall include a disclaimer as part of the e-mail signature, and shall consist of the following language that is automatically inserted by Lotus Notes / Domino server at the end of each message that is sent outside the County:

  CONFIDENTIALITY NOTICE: This electronic communication with its contents may contain confidential and/or privileged information. It is solely for the use of the intended recipients(s). Unauthorized interception, review, use, or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, or authorized to receive for the intended recipient, please contact the sender and destroy all copies of the communication. Thank you for your consideration.

Electronic communication ***messages*** are documents sent or received by a computer system. This definition includes: 1) the contents of the communication, 2) any transactional information, and 3) any attachments associated with such communication. Thus, electronic communication messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

1.8.2 Personal Use

Incidental personal use, if authorized by the appropriate department head, of the County's electronic communication system is permitted as long as it is not excessive and does not degrade the performance of services or interfere with the County's normal business practices and the performance of the County User's business tasks. County Users should exercise sound judgment and sensitivity to others when exchanging personal messages in the workplace.

Lotus Notes is the County standard e-mail system.

- All incoming e-mail must be addressed to the County User's County-supplied electronic communication address such as John.Smith@edcgov.us. firstname.lastname is the Standard Naming Convention.

- Receipt of non-County addressed e-mail via Internet based Internet Service Providers (ISP's) (jsmith@hotmail.com or comcast.com for example) is allowed; however, such email must be accessed via the Internet. Personal attachments may not be stored on County storage devices.

- Examples of County incoming e-mails include those ending with edcgov.us, co.el-dorado.ca.us, edso.org, or /PV/EDC or /SLT/EDC (Lotus Notes addresses).

- The use of Internet-based commercial instant messaging products such as AOL Instant Messaging, Windows Instant Messaging, MIRC, IRC, etc. is prohibited over the County's network.

- Some electronic communication clients allow the use of downloadable plug-ins, allowing the computer user to add "emoticons" and other animations to their electronic communication. The downloading, installation and use of any of these items is prohibited on County computer systems.

1.8.3 State and Federal Laws

Use of the County's electronic communication system is subject to all applicable Federal and State communications and privacy laws. In particular, County Users need to be aware that

attaching programs, sound, video, and images to electronic communication messages may violate copyright laws, and data files containing County User or citizen information are subject to all privacy laws.

1.8.4 Restrictions

Electronic communication may not be used for:

- Unlawful activities.
- Advertising (unsolicited electronic communication commonly referred to as “Spam”).
- Mail "bombs”.
- Uses that violate departmental, County, State or Federal policies, such as, but not limited to, obscenity, sexual harassment, hostile work place, etc .
- Any other use which interferes with computing facilities and services of the County.

The list of restrictions is indicative rather than inclusive of restrictions and electronic communication may not be used for reasons other than those specifically mentioned.

1.8.5 False Identity

County Users shall not employ a false identity in sending electronic communication or alter forwarded electronic communication out of the context of its original meaning.

1.8.6 Representation

County Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the County unless they are appropriately authorized, explicitly or implicitly, to do so.

1.8.7 Network Capacity

The County’s electronic communication system shall not be used for purposes that could reasonably be expected to cause, either directly or indirectly, excessive use of network service or capacity, or cause interference with other County Users use of electronic communication systems, or any computing facilities or services.

For example, attaching files larger than 5 MB to an e-mail message and sending the e-mail to multiple recipients. Files meant to be shared or accessed by multiple County Users should be stored on a shared drive and a file path (link) to the file should be sent to the intended recipients.

1.8.8 Possession

County Users are not responsible for “electronic communication in their possession” when they have no "reasonable” knowledge of its existence or contents.

Preservation of electronic communication (subject to litigation) is required when an individual knows or should reasonably know, by official notification or other communications that the probability of litigation exists or the process of discovery pursuant to litigation exists. Electronic communication and any associated attachments shall be preserved by all reasonable means until notified in writing by County Counsel that the litigation period has

passed and that electronic communication pertaining to litigants no longer needs to be preserved. Preservation may include any and all electronic communication relating to possible litigation being copied onto readable media and delivered (with signed receipt) to County Counsel for later use. By not exercising reasonable and prudent precautions in preserving potential evidence, including electronic communication, you may subject yourself to criminal liability.

Every County User has a duty to preserve evidence in litigation. Destroying documents relevant to threatened or ongoing litigation may result in legal actions against that County User and against the County.

1.9 Use of the Internet

County User's incidental personal use of the Internet, if authorized by the appropriate department head, shall not encroach on or displace time spent performing their work duties. County Users shall not use the Internet in any way that may violate any other County rules, regulations, policies, procedures or practices, or bring civil or criminal liability or public reproach or any conduct tending to bring the County service into disrepute.

1.10 Computer User ID's and Password

All County Users shall be assigned "User ID's" and passwords. Based on a County User's responsibilities and his or her department head's authorization. The County User may be provided with access levels which allow him or her to view, create, alter, delete, print, or transmit information.

County Users are responsible for maintaining the security of their personal account passwords and may not release it for use by any other individual.

All user-level passwords (e.g., electronic communication, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months. There are some systems, such as access for DMV records, that require passwords be changed more often. Please see Section 3.2, Passwords for the correct construction of passwords.

User accounts (e.g., root, enable, NT admin, application administration accounts, etc.) that have system-level privileges or administrative privileges must have strong unique passwords (8-12 character minimum) and will face regular mandatory password changes of no more than every four (4) months.

Passwords must not be inserted into electronic communication messages or other forms of electronic communication, including programming languages.

Any County User found to have violated this policy shall immediately have their access revoked and may be subject to disciplinary action.

Please see General Usage Standards and Guidelines – 3.2 Passwords in support of this policy. All user-level and system-level passwords must conform to the guidelines described in Section 3.2.1, Password Construction Guidelines.

1.11 Computer Viruses

The computer industry faces a continuing onslaught of malicious viruses, worms, malware and other damaging programs that attack computer and network resources. The County maintains equipment and software that reduces the potential impact of viruses, worms, spam, malware and phishing attacks in order to minimize impact of these invasions. It is the responsibility of the County User to take precautions to protect his/her computer and all network resources throughout the County.

Any computer or peripheral connecting to the El Dorado County network must use County approved anti-virus software. This software must be configured to receive regular software and virus signature file updates. All County computing equipment or peripherals, as applicable, shall run up to date versions of the County approved antivirus software or operating systems as approved for distribution by the I.T. department.

County Users should be cautious of opening electronic communication. Viruses can also be received from persons known to the recipient. If there is any doubt as to the validity of an attachment or the electronic communication, County Users shall delete the electronic communication and/or the attachment.

County Users may not download any software, including screensavers, from the Internet without prior authorization from the Director of I. T., or designee.

Computers may not simultaneously connect to the County Wide Area Network (WAN) and other networks such as commercial, private, personal or direct Internet connections via dial-up, DSL or broadband connections.

Critical data should be maintained on servers for security, anti-virus protection and to ensure data integrity through system tape back up.

All computers connecting to the County network are required to be current on all operating system, browser, Office Suite and application updates. These are the updates to the programs mentioned, not necessarily the most current release of the programs.

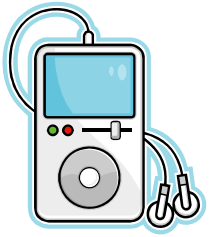
1.12 Removable Data Storage Devices

There are many forms of removable data storage devices in use today. These devices include, but are not limited to; floppy disk, CDs, DVDs, USB storage devices, MP3 players and cameras being the most common. These devices can easily spread malware (malicious software), viruses, worms, etc. to County computer equipment and network. To prevent the spread of malware adherence to the following guidelines is required:

- Floppy drive use has been permanently discontinued.

- Data on CDs and DVDs and USB devices are automatically scanned for malware upon insertion and opening of the files contained therein.

- County digital cameras connected to County computers via docking stations pose little risk and are authorized. Personal digital cameras used in the conduct of County business are authorized to upload digital images.



- MP3 players (IPOD's, etc) may not be connected to County computing equipment. The downloading of music from the Internet to County computers is prohibited. Downloading music at home to MP3 players and connecting to County computers is prohibited due to the very high risk of infection.

- Access to "shared resource" download sites and us of software such as LimeWire and others like it using County computers is prohibited as hackers have no problems obtaining any piece of data off your computer including Personally Identifiable Information (PII). Then they can and will use this information to destroy your credit record and life as reported by all major news agencies.

- All USB based storage devices shall be equipped with integral password protected encryption or Pointsec encryption. Departments processing protected classes of information shall use Pointsec Portable Media Encryptions (PME) to protect data. Implementation of this policy shall be incremental with the acquisition of new USB devices due to budget constraints.

1.13 Portable Computing Devices (WPDA, PDA, Laptops, Tablets)

Portable computing devices such as wireless and/or standard personal digital assistants and laptop computers are subject to every element of the Computer and Network Resource Usage Policies.

Due to their portable nature they are much more prone to loss or theft. Users of these devices are required to practice due diligence in loss prevention of the physical device and data contained within.

The following practices must be observed when transporting or using these devices at work or in the field:

- Physical security is one of the most important aspects of protecting these devices. Never let them out of your sight or leave them any place unattended.

- If these devices must be left in a vehicle, store them in the trunk or other secure location, camouflaging them as necessary to keep them out of sight.

- These devices should be protected with their integral security systems:

- Laptops with Biometric devices (finger print scanners, retinal scanners) or smart cards should be used whenever possible, especially equipment containing sensitive or regulatory protected data. All laptops must be equipped with Computrace theft and loss recovery software.

- Sensitive data should be stored on secured servers as much as possible. Data stored on local hard drives or portable media devices shall be encrypted and password protected.

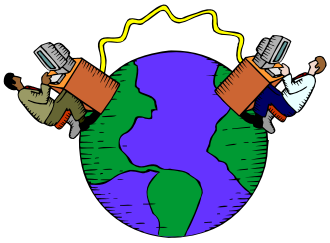
- All portable computer devices must have appropriate County antivirus software installed and County approved firewall software for devices connecting to Internet services to protect data from hackers.

- Wireless Personal Digital Assistants may only communicate with the County e-mail system through the I.T. approved gateways into the Lotus Notes/Domino e-mail system. County approved devices include, Blackberry and Windows Mobile 5 or 6 digital assistants. Palm devices will be phased out as they reach end of life and will not be supported after that point as the gateway that supports Palm OS devices will be discontinued.

- Data from unknown sources may not be beamed to your portable devices via infrared ports.

- Devices that are lost or stolen must be immediately reported to your supervisor and I.T..

1.14 Remote Access



This policy applies to County Users utilizing remote services to access the El Dorado County network. This policy applies to all implementations of remote access that are directed through a VPN concentrator, firewall-to-firewall access, or dial-up service to access County network resources.

If approved by the appropriate department head or authorized representative (if user is not a County employee) and the County Security Officer, remote access users (County Users, outside government agencies, contractors, vendors, etc.) may utilize the benefits of remote access, which is a "user managed" service. Remote access users will be responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. When connecting to County hosted remote access services, the remote access user is responsible for any and all toll charges associated with the use of remote access equipment.

The following policies apply to remote access users:

- It is the responsibility of remote access user with remote privileges to ensure that unauthorized users are not allowed access to El Dorado County internal networks.

- When actively connected to the County network through dial-up services, all other connections to non-County networks must be disconnected.

- Remote access accounts will be created and managed by El Dorado County I.T.

- All computers connected to El Dorado County internal networks via remote access are subject to the same security requirements as those connected to the County network.

- Remote access County Users will be automatically disconnected from El Dorado County's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network.

- VPN connectivity will be through approved client software or other connectivity methods as defined by El Dorado County I.T.

- When authorized for remote access to the County network using personal equipment, County Users must understand that their machines are a de facto extension of El Dorado County's network, and as such are subject to the same rules and regulations that apply to El Dorado County-owned equipment, and their machines must be configured to comply with the security policies and standards of El Dorado County.

- When authorized for remote access to the County's network, County Users have unique access to sensitive resources. To insure network security, it is critical that all remote County Users actively support and fully comply with the measures described in these policies. Failure to comply can place the entire County network at serious risk and could lead to disciplinary action.

- Remote access users are required to complete a remote access request form, provided by I.T., which identifies security, antivirus and other computer protection requirements for the requesting party's access. The form must be signed by the department head, or authorized representative if not a County employee, and the Security Officer. After submission of the completed form, I.T. will ensure remote systems meet County specifications prior to granting access to the County network.

COUNTY USER AGREEMENT

El Dorado County Computer and Network Policies Agreement

I have read and understand that:

1) As a user of the County's information technology resources, I may have access to sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all users actively support and fully comply with the measures described in the Computer and Network Resource Usage Policies and Standards Guide. Failure to comply can place the entire County network at serious risk. Failure to comply may subject me to disciplinary action.

2) As a user of the County's information systems I shall at all times act in accordance with all applicable laws and County policies, rules or procedures. I shall not use County information technology resources in an improper or unauthorized manner.

I have received, read and am fully aware of the El Dorado County Computer and Network Resource Usage Policies and Standards Guide. I agree to comply with the terms of this policy.

User Name: _____

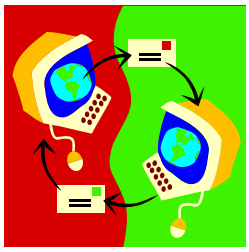
Signature: _____

Date: _____

This form shall be signed on an annual basis and be retained in the department, district or agency file.

GENERAL USAGE STANDARDS AND GUIDELINES

3.1 Electronic Communication



The County encourages the use of electronic communication to enhance communication and business activities. Standards are necessary to ensure the appropriate use of electronic communication and to prevent or limit disruptions to work activity and computer services.
The nature of electronic communication at the present time makes it susceptible to misuse. County Users need to be aware that sensitive or private information can be easily forwarded to other individuals the originator never intended, both internal and external to the County.

Users of the County's electronic communication services need to be aware that use of these services is a privilege granted with the expectation that it will be used for business purposes and in a professional and courteous manner similar to other forms of communication. All electronic communication sent or received by individuals through County User's accounts is the property of the County and may be examined by County officials at the request of a County User's department head and with approval from the Director of Human Resources.

It is important to understand and use electronic communication appropriately within the County use policy and your specific departmental electronic communication use policy. Additionally, for a guide to safe electronic communication use please refer to the EDCNET, the County's intranet website:

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

All e-mail, whether it is a new e-mail or it is a response, shall contain the e-mail security disclaimer as defined in Section 1.8.1 of this document.

3.1.1 Security and Confidentiality

The confidentiality of electronic communication cannot be assured. County Users should exercise extreme caution in using electronic communication to communicate confidential or sensitive material. Any electronic communication that contains protected classes of information (HIPAA, PII, PHI Sarbanes-Oxley, etc.) must be encrypted before it is electronically communicated.

3.1.2 Anti-Spam Measures

Never respond to a spam electronic communication. Many spam electronic communications may contain instructions on how to remove your address from their address list. More often than not, your response only confirms they have a valid address. They will continue to send you spam and will sell or share the now confirmed active address to other spammers.

Never use your County electronic communication account for Internet purchasing, auction sites (EBay etc.) or supply your County Internet e-mail account address to suspicious or untrusted sites.

El Dorado County has made a significant investment in technologies designed to minimize our exposure to spam and viruses. This equipment will quarantine suspicious electronic communication. The equipment uses a series of anti-spam /antivirus measures to assign a point value to incoming e-mail. When an electronic communication hits these thresholds it

is normally quarantined. Often times, incoming electronic communication may be quarantined due to poor maintenance and/or security measures at the senders end, causing their electronic communication services to be “blacklisted” and resulting in quarantine at our servers. These actions are by design and meant to protect our systems and your County computers.

The process of e-mail quarantine may delay the delivery of electronic communication. I.T. staff checks quarantine areas regularly to minimize the impact on County staff members. Although this quarantine process may at times be inconvenient, it is necessary to prevent the entry of un-wanted and potentially dangerous electronic communication into the County system.

3.1.3 HIPPA and Compliance with Electronic Communication Privacy Act

Standards are under development to comply with above regulations and acts. In general, electronic communication under the umbrella of these regulations requires data and electronic communication encryption. The County has adopted hard drive, USB portable media and e-mail encryption standards. The I.T. department will work with departments subject to these standards to ensure compliance shall be in place by July of 2010.

3.1.4 E-mail Retention

Formal e-mail retention policies are under review and will be complete in the near future; after the appropriate review and approval processes. E-mail retention policies differ from e-mail archiving. Archiving manages the size of e-mail files. Retention manages the age of e-mail and deletes e-mail that age past a certain date.

3.1.4.1 Account File Size Restrictions and E-mail Retention Standard

E-mail attachments can consume large amounts of storage space on County file servers. It is recommended that attachments be detached and stored on a local computer or stored on a server and deleted from electronic communication to preserve electronic communication server storage.

County User best practices should include proper management of their e-mail. Departments must develop guidelines pertinent to their business requirements that dictate how long specific electronic communications should be kept, what can be deleted and when. Departments undoubtedly have differing needs for retention based on Local, State, and Federal law as well as accepted best practices within their industries.

A departmental e-mail retention standard must be designed to reflect the need for each County User to manage his or her e-mail effectively and efficiently. This standard will help minimize the impact on County resources in storing and managing the County's enterprise e-mail system.

The maximum e-mail file size is set at 300 Mb. When a County User’s file size reaches 250 Mb the user receives an e-mail notification that their e-mail file is reaching the maximum allowable size. If the file size reaches the 300 MB limit send\receive e-mail privileges are suspended until files are deleted or archived to bring the file size below the maximum allowable size. Contact I.T. for assistance with archiving your e-mail.

3.1.5 Managing E-mail

You may receive and manage your 'production' e-mail file and create folders as you wish and according to your department's policy.

You can manage your e-mail by:

- Deleting e-mail you no longer need.
- Saving only e-mail that you are required to save by department policy or based on legal requirements, to a designated archive folder(s). This process will move your 'archived' e-mail from your 'limited' production area to your archive storage location.
- Removing attachments from e-mail and store them on local computer and/or server storage.
- Printing your e-mail and saving the printed copy (or make Adobe 'PDFs') and then deleting the e-mail.
- Once a County User no longer needs an e-mail and moves the e-mail to the Trash folder the e-mail is held in the Trash folder for 96 hours then deleted. By deleting all e-mail in the Trash folder the County User ensures all messages are deleted. Reductions to the size of the County User e-mail account after deleting e-mails may not immediately reflect the accurate size for up to two days due to automated processes. If a County User requires the size change to take immediate effect due to reaching the 300Mb limit, contact the Help Desk.

These processes should help bring e-mail file sizes below the allowable limits.

3.1.5.1 Archiving E-mail

E-mail archiving guidelines are still under discussion at this time.

3.1.5.2 Backup Process for Production E-mail and Archived E-mail

- Production e-mail will be backed up daily (normal business day).
- Production e-mail will be backed up to tape on a weekly basis for 'off-site' disaster recovery purposes.

3.1.5.3 E-mail Account Deletions

All Internet electronic communication is forwarded to the County e-mail system, Lotus Notes. Upon notification by a department head or Human Resources that a County User is confirmed to have permanently left County service, the Internet account will be frozen or deleted. The County e-mail files are moved to “obsolete” and the County User’s name is removed from the County e-mail list. Files placed in “obsolete” are retained for 60 days and then deleted. Departments requiring any deviation from this standard should immediately contact the Director of I. T. to avoid deletion of files intended for an extension of time prior to deletion.

3.1.5.4 Anti-Virus Measures and E-mail Attachments

Never open any file attached to an electronic communication from an unknown, suspicious or untrustworthy source. Delete these electronic communications immediately, then "double delete" them by emptying your Trash. One of our best lines of defense against malicious attacks is the computer user. Regularly check electronic communication for notifications sent to you by I.T. regarding viruses and electronic communication “scams”. An informed computer user is an aware user and can better identify suspicious content in electronic communication.

Delete spam, chain, and other junk electronic communication without forwarding.

Never download files from unknown or suspicious sources or websites. Never visit "underground" sites, hacking sites, or any site that is not required in the execution of your duties as a County User. These sites can put the integrity of the County network at risk through malicious code, either intentionally or unintentionally.

Avoid direct disk sharing (peer to peer) with read/write access unless there is a business requirement to do so.

3.1.6 Electronic Communications – Instant Messaging

The County is using Lotus Instant Messaging as an additional form of electronic communication between County Users. All policies applicable to electronic mail apply to electronic messaging. Special precautions must be observed with the use of instant messaging due to the nature in which transcripts of instant messaging are logged. The default for Lotus Notes Instant Messaging is "not logged".

Should any County User receive objectionable, offensive or threatening content during an instant message session, it is important to follow these procedures:

- Do not close the instant message session or turn off your computer
- Contact your supervisor to report the behavior in question

As applicable, your supervisor will take the appropriate action, up to and including contacting the Human Resources department who will direct the collection of the data in question, following strict confidentiality guidelines.

3.2 Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of El Dorado County's entire corporate network. As such, all El Dorado County Users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this standard is to establish criteria for creation of strong passwords, the protection of those passwords, and the frequency of change. This includes all County Users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any El Dorado County facility, has access to the County network, or stores any non-public County information.

3.2.1 Password Construction Guidelines

Passwords are used for various purposes in El Dorado County. Some of the more common uses include: personal computer accounts, network server accounts, web accounts, electronic communication accounts, screen saver protection, voice electronic communication password, and mainframe accounts.

Poor or weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "El Dorado County, “County”, "EDC", or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong or effective passwords have the following characteristics:

- The password contains at LEAST 8 characters.
- The password contains both upper and lower case characters (e.g., a-z, A-Z)
- The password has digits and punctuation characters as well as letters (e.g., 0-9, ! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , . /)
- The password is not a word in any language, slang, dialect, jargon, etc.
- The password is not based on personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do **NOT** use either of the above examples as passwords!

3.2.2 Password Protection Standards

Do not use the same password for El Dorado County accounts as for other non-County access (e.g., personal ISP account, EBay, personal electronic communication accounts, etc.). Do not share El Dorado County passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential County information.

Here is a list of password “don’ts":

- Don't reveal a password over the phone to un-authorized personnel.

- Don't reveal a password in an electronic communication message.
- Don't reveal a password to the manager without a written request for such information from your manager.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.
- Don't use the "Remember Password" feature of applications (e.g., Internet Explorer, Outlook, Outlook Express, and Entourage).
- Don't write passwords down and store them anywhere in your office.
- Don't store passwords in a file on ANY computer system (including PDA's) without encryption.

All computing equipment deployed in El Dorado County shall have screen savers with password protection enabled and set to lock the computer after ten (10) minutes of inactivity. County Users should hit "Ctrl/Alt/Delete keys and lock their computers to protect against un-authorized access whenever leaving their work station.

If someone demands a password, refer them to this document or have them call the Director of I. T.. Departments needing authorized access should contact the Information Technology department to securely address this need.

If an account or password is suspected to have been compromised, report the incident to I.T. immediately and change all passwords.

3.2.3 Application Development Password Standards

Mainframe applications should use RACF security functionality. Client-server and web-based applications should use Active Directory Services security functionality.

3.2.4 Pass Phrases

Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks."

A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass phrase:

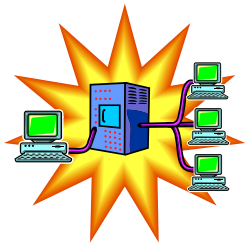
"TheTrafficOn50WasTerribleThisMorning"

All of the rules above that apply to passwords apply to pass phrases.

3.2.5 Use of Passwords and Pass Phrases for Remote Access Users

Access to the El Dorado County networks via Virtual Private Networking (VPN) access and some networked resources are controlled using the username/password (challenge/response) mode of authentication. Access to the County network via VPN is tightly controlled.

3.3 Server Storage Utilization



To maximize server storage, County Users should properly manage their data and directory structures. There are several methods of file storage and associated back-up. The recommendations in the next section provide options and recommendations for file storage, directory structure and back-ups to ensure the availability of server storage space.

3.3.1 File Storage Options

- Operating system and applications are loaded on the desktop computer and all data files stored on the local machine hard drive. *This option provides local access to the computer data files, but offers no backup of those files. Hard drive failure will result in complete loss of data files.* ***This option is <u>not recommended.</u>***

- Operating system and applications are loaded locally and all data files are stored on a network server. *This option safeguards data in two ways: 1) data files reside on servers, 2) data files on servers are backed up to tape nightly. A possible drawback to this option is the inability to access data on the server in the event of server or network problems.*

- Operating system and applications are loaded locally. All data files are stored on the local hard drive and its directory structure configured to allow for scheduled copying of local data files to the server. *This option safeguards data in three ways: 1) data files reside on local drives, 2) data files reside on server hard drives, 3) data files are backed up to tape nightly. In the event of network or server problems, data files stored locally will be available. While this method requires the largest amount of user intervention due to regularly scheduled backups of local data files to server drives, it does provide maximum availability and protection of data files.*

- "Thin Client" computer; all files reside on a server. The operating system and applications run at the server level, data files are stored on server drives. Proper file management at the server level preserves hard drive space.

3.3.2 Server File Storage

- The majority of County computers are connected to Windows based servers. These servers store data files and send print jobs to networked printers. Storage must be managed to maximize storage capacity.

- Server hard drive arrays have finite capacity. NEVER copy the entire contents of local drives to server drives. This wastes server-based storage.

- County User-specific data files should be copied only to the County User's server home directory which is normally designated as the "H:" drive.

- Data files common to a group should only be copied to the "shared" server directory's appropriate sub-directory. Always store data files in the appropriate sub-directory as defined within your department and/or group. NEVER store data files at the root of shared directories.

- Do not store multiple copies of data files on a server. There is no need to have a copy of the same file in your home directory and a group directory. Do not de-compress operating system or application service packs or updates to server hard drives.

- Clean up your directories at least monthly. Delete old data files or files no longer needed and remove unnecessary iterations or versions of data files. Server storage is not to be used for storing non-work-related music, video, or picture files.