County of El Dorado

Procedures and Guidelines

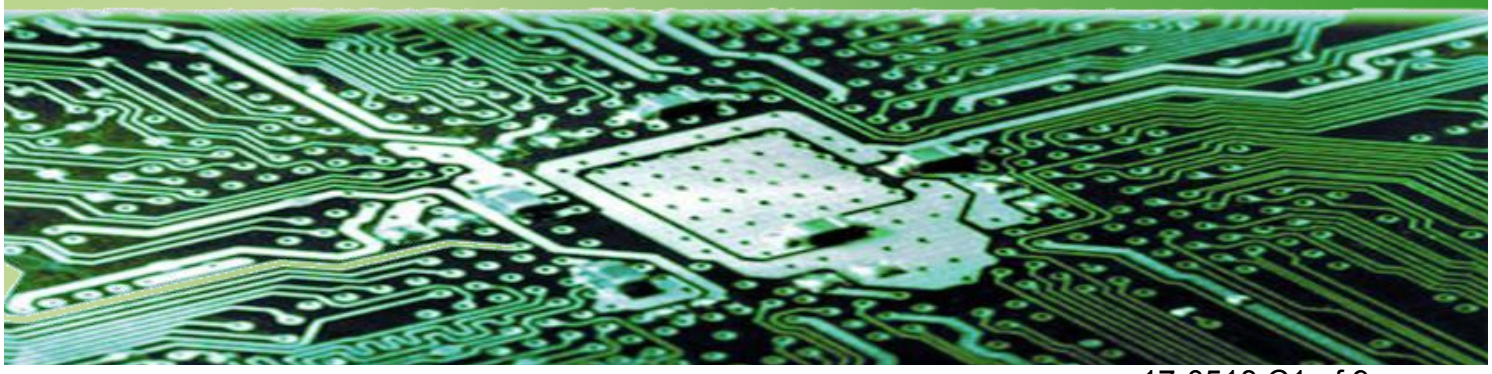
Information Technologies

Version 1.0

July 2017

General Network Usage

Procedures and Guidelines



Document Change Record

Effective Date	Section(s) Changed	Comments
18 July 2017		Initial publication

Contents

1. PURPOSE

This document contains procedures and standards regarding the use of County network resources, in support of the General Network Usage Policy (published in compliance with Board Policy A-19).

2. DEFINITIONS OF TERMS

Information Domain – the entire communications infrastructure (hardware, software, and data) that comprises the County's information technology network, excluding County communications infrastructure that is specifically for public use (such as the "EDC-Public-Wireless" WiFi network).

Network Resources – collective term for the capabilities and services provided within the County information domain. Examples of network resources include: virtual workstations; PCs; data storage; peripheral devices (printers, scanners, etc.); servers; internet connections; mobile devices (laptops, tablets, smartphones); voice telephony devices; and any other electronic information services accessed by Users in conducting their work.

PHI (Protected Health Information) – information about a person's medical history or condition. PHI is protected from unauthorized disclosure by HIPAA and other Federal laws.

PII (Personally Identifiable Information) – information that can be used to verify the identity of an individual for purposes of conducting financial or other transactions. Disclosure of PII may lead to fraud or identity theft.

User – a person who is granted official access to the County's information domain. This definition includes County employees, contractors, vendors, and other public agency employees such as fire departments, community services districts, and multi-jurisdictional or joint operating authorities.

3. GENERAL NETWORK USAGE PROCEDURES AND GUIDELINES

3.1. Use of Network Assets

Any computer or peripheral device connected to the El Dorado County information domain must be either owned by the County or approved by the Information Technologies Department. All devices must run approved versions of operating systems and applications, must have approved anti-virus protection, and must meet all other technical specifications as determined by the IT Department. Questions about these specifications should be directed to the IT Help Desk.

Users must submit an IT Help Desk ticket to add or delete any device from the network, whether personal or county-owned. This procedure applies to mobile devices and devices used for remote access.

The Help Desk can be reached at ext. 5696. Tickets can also be submitted via the County intranet at http://helpdesk/portal .

3.2. User Privacy

All County workstations display a "consent to monitoring" statement that must be acknowledged by Users when logging in to the workstation. In compliance with Public Records Act and other government transparency regulations, all data on the County information domain must be retained in accordance with the County records retention schedule and may be subject to disclosure. This pertains to all data in the information domain, and may include personal data or data not related to official County business.

The IT Department, with oversight and direction from the Chief Information Security Officer (CISO) will maintain tools and technology that allows search and discovery of County data. Any searches or discovery actions must be approved and directed by Human Resources, County Counsel, or—in the case of Public Records Act requests—the Clerk of the Board.

Users may request IT assistance in searching for or recovering their own files or files they have permission to access. Requests to access or recover files or data belonging to another employee, even if requested by the employee's supervisor, manager, or department head, must be approved by Human Resources. In such cases, the files or data will be screened by Human Resources prior to granting access to the requester.

3.3. User Access Credentials

Access credentials are issued to all Users. These credentials are used to verify the identity and access levels of the User. There are three main types of credential used by the County:

- Something you **know** — Example: a password or personal Identification number (PIN)
- Something you **have** — Example: a building access card or key fob
- Something you **are** — Example: a fingerprint

Users will usually be required to use at least two of the above credential types for access, depending on their position and duties assigned.

3.3.1. Multi-factor Authentication Procedures

Many Users will have an access badge reader attached to their desktop workstation. The proximity reader will sense the presence of a building access card or key fob. To log in, the User will be required to tap their badge or fob on the reader, and then enter a PIN to verify their identity.

NOTE: Although a password is not required for log-in when using the badge reader, the user is still required to create a new password every 60 days. However, the User does not have to use their password for access if they have a badge reader/PIN method.[1]

[1] Some applications and privileged accounts may require passwords or other access credentials.

New Users will be required to follow a registration and PIN creation process upon first log-in. This process is relatively simple, and the log-in software will guide the User through the steps. Users that encounter any problems with registering or logging in should contact the IT Help Desk at extension 5696.

3.3.1.1. Password and PIN Rules

These rules are based on federal and state guidelines and IT security best-practice.

- Users are required to change their passwords every 60 days.[2]
- Passwords must contain at least 8 characters.
- Passwords must contain all of the following:
  - At least one upper case letter
  - At least one lower case letter
  - At least one number
  - At least one special character
- Users may not re-use their 24 most recent passwords
- Users are required to change their PIN every 60 days
- The PIN must contain at least 6 digits

Users can contact the Chief Information Security Officer (CISO) or the IT Help Desk with any questions about password rules.

3.3.2. Shared Workstations

Some workstations and mobile devices require access by multiple Users. (For example, a workstation in a conference room.) Users must log in to the shared workstation using their own credentials, as they normally do. Sharing workstation access is not permitted. Users are prohibited from logging in and allowing another person to use the workstation. Likewise, Users are prohibited from using any workstation that has been unlocked or logged into by another person.

Users should always log out of a shared workstation when they are finished using it.

Users who encounter problems or have questions about logging in to a shared workstation should contact the IT Help Desk at extension 5696.

3.3.3. Protection of Credentials

Users are responsible for protecting all of their credentials (passwords or PINs) from disclosure or compromise. Disclosure of log-in credentials risks the integrity of the entire County information domain.

---

[2] Regulations for certain classes of information may require Users to change their PIN or password more frequently.

Users shall not share or disclose log-in credentials to any other person, including other employees, managers, or County officials. Users should never allow any other person to use their workstation or mobile device while they are logged in to the County information domain.

Users should refrain from writing down their PIN or password and keeping it on or near the workstation. Users shall not transmit their credentials in any email message or by other means, including by phone.

(Note: The County IT Department will ***NEVER*** ask for your password or PIN over the phone or by email. If you receive such a request, it is likely a scam by an outside attacker, and you should report to IT. ***Do not EVER give your password or PIN to someone over the phone or by email!***)

3.4. Use and Ownership of Data

3.4.1. Data Storage Procedures

The County's network storage is closely monitored, and has been sized to meet our business needs. However, network storage capacity is not infinite, and Users should strive to manage their data efficiently. There are several steps Users can take to ensure they are not over-using network storage assets.

Network storage is backed up and protected by a number of IT Department processes, so Users should not make their own "back-up" copies of data that is already in network storage. This includes copying their "home" or H: directory into other network directories, or vice-versa.

Users are encouraged to use their H: (home) directory for data storage instead of storing files on their local hard drive. (Also, files stored in a User's H: drive will still be available if they log in to a different workstation.)

Users should avoid storing copies of files in multiple directories. Users are encouraged to periodically clean up and organize their files and directories.

Desktop and laptop operating systems and applications are managed by IT processes, so it is not necessary for the user to make copies of any operating system or application files.

Users should not use County network storage for personal data or files (including photos, music, video, etc.).

3.5. Use of Personally Owned Software and Equipment

3.5.1. Software License Compliance

Users may not download any software from the Internet without prior authorization from the IT Department or designee. Requests for software installation should be submitted via the IT Help Desk. Requests for software that is not currently licensed for use by the County may require a departmental requisition or purchase.

3.5.2. Copyright Protection

Use of copyrighted material is generally prohibited unless properly purchased or owned by the County. Users shall not install software or store any data on any County network resource (computers or storage) unless the county has licensed use or rights to the software or data.

Use of photos or text from copyrighted sources in County documents (including PowerPoint slides) is strongly discouraged. Users who have questions about use of copyrighted material should contact the IT Department.

3.5.3. Use of Personally Owned Equipment

Users may not connect any personally owned external device to County workstations or networks under any circumstances, unless authorized by the IT Department. This includes USB drives, external hard drives, smartphones, iPads, and tablets. Employees must charge their personally owned devices by connecting directly to power outlets.

3.6. Use of Non-County Devices

County email can be accessed from personal devices. For access from smartphones or tablets, the User will be required to install a remote device management app that will enable remote wiping of the device in the event of theft or loss. The IT Department will assist as necessary. If users choose to access County email through a web browser, remote device management app is not necessary.

Employees should be aware that communications and data, including text messages, related to the conduct of County business that are sent or received using private accounts or maintained on personally-owned devices are considered public records and may be subject to disclosure under the Public Records Act.

3.7. Remote Access

Users may, with Department Head approval, request remote access to the County information domain from a non-County device or location. The IT Department will provide a method of access for all such approved requests via one of two options. The request form for Remote Access is available on the IT Department intranet page. Users can also contact the Help Desk for assistance.

Some cases may require a Virtual Private Network (VPN) connection. Users are required to abide by all County policy and procedures when connecting via VPN, including Section 3.3 and 3.4 of this document.

Most employees will be assigned a Virtual Desktop. Virtual desktops can be accessed securely from practically any device or location, and will be the preferred method of accessing County systems from remote locations or from personal devices.

The IT Department will assist Users in setting up remote access, but will not be responsible for any changes, damages, or loss of data on personal devices that are used for remote access.

3.8. Personal Use of Network Resources

Reasonable use of County workstations and networks for personal communications is permitted. Department policies will vary, but in general, Users may not use County network resources for the conduct of commercial business or private activities that violate County policies on sexual harassment, hostile workplace, or offensive material.

The County IT Department uses a number of tools and systems that block some internet traffic and content from County Users. This is done to protect our networks from malicious attacks and to screen out patently offensive content. If Users have a legitimate need to access content that they believe is being blocked, they should contact the IT Department or CISO to discuss the matter.

Users should not use County network connections to stream video or audio unless it is for County business. Music streaming should be done via personal devices, using commercial carriers.

The County provides public WiFi in some locations. This service is for use by the public while they are conducting business with the County. Employees should not connect their personal devices to the County's public WiFi. This network has limited speed and capacity, and employees who use it for personal devices will impact the quality of service provided to the public.

3.9. Electronic Messaging

Users have the ability to communicate by email, instant messaging (Google Chat), video and audio conferencing services, phone and voicemail. These services are to be used for County business only. Reasonable use of phones and email for personal communication is permitted, but with the same restrictions and guidelines noted in the previous section of this document. (Section 3.8)

All County email is retained by the IT Department for Public Records Act requests and litigation discovery. Users may not access email accounts belonging to other employees. Users are required to manage their own email, and all access credentials must be protected using the procedures in Section 3.3 and 3.4 of this document.

All privacy and security policies and procedures that apply to use of the County network also apply to County telephone system. Users should employ the same level of caution and care with voice communications as they do for email or other electronic messaging. Disclosure of sensitive information, including access credentials, to unauthorized persons is prohibited, regardless if by email or telephone.