County of El Dorado

Procedures and Guidelines

Information Technologies

Version 4.0

July 2023

General Network Usage and Access Procedures and Guidelines

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

Data Classification - Department identifies its data for the purpose of defining its value, location, and level of protection. Example Classification levels include Confidential, Internal, and Public.

Data Owner: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

External Trusted Partner - a person who is granted official access to the County's information domain. This definition includes contractors, vendors, and quasi-governmental employees such as fire departments, community services districts, and multi-jurisdictional or joint operating authorities.

Information Domain – the entire communications infrastructure (hardware, software, and data) that comprises the County's secure network. Differentiated in this policy from County communications infrastructure that is specifically for public use (such as the EDC-Public WiFi network).

Kiosk – A computer that is accessed by more than one user with no user credentials required. The common use of a kiosk is for public access to make a transaction or look up information.

Network Resources – collective term for the capabilities and services provided within the County information domain and cloud environments (Examples listed in the A19 Policy).

Protected Data - Applies to data that must be kept secure under State, Federal, County, Tribal, and Local regulations which includes:

PII - Personally Identifiable Information
HIPAA - Health Insurance Portability and Accountability Act
CJIS - Criminal Justice Information Systems
PHI - Protected Health Information PCI - Payment Card Information

Shared Workstation – A computer that is accessed by more than one user. Each user must access the computer with their user own user credentials. The common use of a shared workstation is in coworking spaces and shared office spaces.

Team Owner – User assigned to an MS Team that can manage access and control to the team.

User – a person who is granted official access to the County's information domain. This definition includes employees, contractors, vendors, and quasi-governmental 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.

3.1.1 Operating System and Applications

All devices must run approved versions of operating systems, software, and applications, must have approved End-Point protection, and must meet all other technical specifications as determined by the IT Department following Computer & Network-Based Information Systems Policy A-13. Questions about these specifications should be directed to the IT Help Desk.

3.1.2 Security Updates

All County devices must be connected to the network and powered on for mandatory weekly security updates. This includes assigned devices, shared devices, and devices in conference rooms. Users Teleworking need to follow guidelines in Telecommuting Policy E-12.

3.1.3 Adding and Assigning a Device

Departments must submit an iSupport ticket when adding, assigning, moving a device, or reassigning a user to a device.

3.1.4 Removing a Device (Surplus)

Departments must submit an iSupport ticket when removing a device. Devices must follow the IT data destruction procedures.

3.1.5 Telecom Equipment

Departments must submit a Telecom ticket for all phone installs, transfers, moves, and removal of equipment. This includes installation of cabling.

3.2. Data Access

All County workstations display a “consent to monitoring” statement that must be acknowledged by Users when logging in to the workstation. This pertains to all data in the information domain, even personal information, not related to official County business. In compliance with Public Records Act and other government transparency regulations, data stored on the County information domain is considered discoverable.

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 Department Heads, Human Resources, or County Counsel.

3.2.1. Request for Own Files

Users may request IT assistance in searching for or recovering their own files or files they have

permission to access within the County backup procedures.

3.2.2 Supervisor Access

- **Active Employees**
  - OneDrive: Employees can share content with their supervisor.
  - Email: Employees can delegate access to their supervisor.
  - H Drive: IT can provide access to the supervisor upon request.

Note:
Department head approval is required if a supervisor is requesting access to any of the above without the employee's consent or knowledge.

- **Inactive Employees**
  - OneDrive: Supervisor (as defined in Active Directory), by default, will have 30 days to review content in an employee's OneDrive.
    - After the 30 days the employee's OneDrive is automatically deleted. If the supervisor would like to retain any items, they must be moved out of the employee's OneDrive during the 30-day window and stored in a separate file location.
  - Email: If requested in the termination process, supervisors can have access to the employee's mailbox for 30 days.
    - If access is not requested during the termination process, the only way to view this content is with eDiscovery software tool and the department must submit an iSupport ticket to request IT assistance to search and view emails. The request must be approved by either the department head, County Counsel, or Human Resources.
  - H Drive: If requested in the termination process, supervisors can have access to the employee's H Drive for 30 days.
    - If access is not requested during the termination process, the H Drive can be restored from backup for up to six months, post termination.

3.2.3. Request for Another Employee's Files and Mailbox

- **Active Employees**

Active employees can share or delegate their own files and mailbox as needed (as permitted within department policy and process needs). If the files and mailbox are not shared or delegated by an active employee, request to access or recover the files and mailbox of another active employee must be approved by the employee's department head, County Counsel, or Human Resources.

- **Inactive Employees**

Requests to access or recover files or data belonging to another inactive employee must be approved by the employee's department head, County Counsel, or Human Resources prior to granting access to the requester.

3.3. User Access Credentials

Each El Dorado County employee shall have a uniquely assigned user ID to enable individual authentication and accountability. Documented authorization from the employee's supervisor is required for the user ID to be issued and removed. Additional documentation and HR approval is required for user ID name change request. It is the department's responsibility to notify IT using an iSupport ticket for all employee transfers and employee terminations.

Each trusted external user (contractor, vendor, volunteers, outside agencies) shall have a uniquely assigned user ID to enable individual authentication and accountability. An External Trusted User form must be completed to define use and access level with authorization from the El Dorado County – department head prior to the user IDs being issued. The Information Security Office (ISO) will perform an annual audit and will monitor expiration dates. Access can be removed by the IT department if the External Access form is not renewed for access.

Users are required to manage their own access credentials, and all access credentials must be protected using the procedures specified in this Section 3.3.

3.3.1. Passwords

These rules are based on IT security best-practice based on NIST.[1]

Users are required to change their passwords every 90 days.

- 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

User will be locked after 5 password attempts.

3.3.2. Multi-Factor Authentication (MFA)

All users (employees or trusted external users) are required to engage in one additional authentication beyond username and password to access County resources when off network.

3.3.3. 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

[1] Regulations for certain classes of information may require advanced password protect i.e., Department of Child Support Services (DCSS) must meet Section 6002 - Password Standards

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.

3.3.4. Kiosks

IT can create a kiosk device. Kiosks are shared devices and are typically configured to allow only minimum required access. IT will evaluate the business requirements on a case-by-case basis and if suitable, develop a kiosk profile for the requesting department.

3.3.5. Protection of Credentials

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

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 a scam by an outside attacker. ***Never provide your password or PIN to someone over the phone or by email!***)

3.3.6 Password and MFA Resets

Users can change or reset passwords using M365 Self-Service Password Reset (SSPR), with no administrator or help desk involvement. If a user's account is locked or they forget their password, they can follow prompts to unblock themselves and return to work.

If the IT department is required to reset the user password or remove an MFA method, the IT department must verify user. Approved methods to verify users are listed below.

a. User needs to validate information from last Personnel Action Form (PA)

b. User can come onsite to the IT department

c. External user's passwords will be reset using the call back to the number on file from the Trusted External User form.

3.3.7 Temporary Password Usage

Temporary passwords are allowed with an immediate change (15 mins) to a permanent password.

3.4. Use and Ownership of Data

3.4.1. On Premises 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.

User Guidelines

- 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.)

Local Drive Guidelines:

- Users should not use their local hard drive. Local hard drives are NOT backed up by the IT Department.

Shared Drive Guidelines:

- Departments data owners or designee must approve access to department shared drives.
    - If a data owner is not assigned IT will assume the user requesting access has authority. Users can not request access for themselves.
    - Departments may not request access to another departments shared drive without the department head approval of the shared drive.
    - Departments are responsible for shared drive access for employee onboarding and offboarding.
    - Departments will open iSupport tickets for shared drive access and access removal.

Departments should review shared drive files and directory for cleanup and use annually.

3.4.2 M365 Data Storage Procedures

M365 storage capacity is not infinite, and users should strive to manage their data efficiently.

OneDrive:

- Users are encouraged to periodically clean up and organize their files and directories.
- User should share OneDrive documents with the understanding of the security risks and data protection guidelines.
- Users should understand when agreements need to be in place to share protected data with departments and external users. Best practice is to use MS Teams to share with external users.
- Users are required to use sensitivity labels when required by regulations to protect data.

MS Teams:

- Users will be placed and removed into department MS Teams during on boarding and off boarding once posted by payroll
- MS Teams owners must approve and add users to MS Teams. MS Team owners need understand security risks and data protection guidelines.
- MS Team owners need understand when agreements need to be in place to share protected data with departments and external users.
- MS Team owners must remove users from MS Teams for transfers and off boarding
- MS Team owners need to review external users for use and off boarding
- Team owners and Team members are required to use sensitivity labels when required by regulations to protect data.

3.4.3 Cloud Storage

All additional types of cloud storage must to be approved by IT in alignment with Computer & Network Based Information System Policy A-13.

3.4.4 Portable Data Storage Procedures

Portable data storage (i.e., USB drives) is not allowed unless approved by IT. The preferred method of data transfer is Secure File Transfer (SFTP).

- The USB Drive must be labeled, encrypted, and handled according to its data classification.
- Users need to have a data sharing agreement with external users on file when providing data
- Data transfers outside of controlled areas must be approved and tracked by the data owners. All activities associated with transfers and transport needs to be documented.

- The data stored on portable storage device must be removed and/or sanitized once usage is no longer required.

3.4.5 Data Transfer Storage

User may request Secure File Transfer (SFTP) to transfer files and sensitive data minimizing the risk of exposing data to unauthorized parties. Regulations such as HIPAA, set a standard for secure file transfer. Failure to comply with these standards can result in substantial penalties. Many data protection regulations specify the need for encryption when transferring sensitive files. SFTP makes it easy to comply by including encryption as a default security measure when transferring data.

- Users need to have a data sharing agreement with external users on file when providing data

- SFTP is a temporary storage. Users requesting SFTP must provide a data retention timeline or IT will automatically default to a 30-day data retention unless the department has a business requirement.

3.5. Use of Personally Owned Software and Equipment

3.5.1. Software License Compliance

Users may not download any software or use cloud software without prior authorization from the IT Department or designee. Requests for software installation, or cloud use, should be submitted via the IT Help Desk. Requests for software that is not currently licensed for use by the County must follow Computer & Network-Based information Systems Policy A-13 and 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.

Users who have questions about use of copyright 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. This includes USB drives, external hard drives, smartphones, iPads, and tablets. These devices may not be connected under any circumstance, even for charging. Employees can charge their personally owned devices by connecting directly to power outlets.

Employees should be aware that any official government data, including text messages, present on personally owned devices are subject to search and discovery for Public Records Act requests. In short, this means that if an employee uses a personal smartphone, laptop, or tablet for County business, they may be required to allow access to their personal devices to be

searched by County or other government officials.

3.6. Remote Access

Employees may, with Department Head approval, request a VPN account for remote access by the Telework form or Job Class Remote form. Employees must abide by all County policy and procedures when connecting via VPN, including General Network Usage Policy A-19 and Telecommuting Policy E-12.

The IT Department will assist Users in setting up remote access on County issued devices.

3.7. Personal Use of Network Resources

Users may not use County network resources for the conduct of commercial business or private activities that violate County policies on 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 content deemed to be offensive or against the public interest. 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 Wi-Fi in some locations. This service is for use by the public while they are conducting business with the County. 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.

Users are not allowed to use County email accounts for personal use, for e.g., creation of iTunes accounts using County email accounts on mobile devices.

3.8. Electronic Messaging

Users have the ability to communicate by email, Team chat, Team posts, video and audio-conferencing services, phone and voicemail. These services are to be used for County business only.

All County emails, Team chats, Team posts, videos, cloud documents and audio-conferencing services, phone and voicemail are retained by the IT Department consistent with the County's retention schedule and may be subject to disclosure for Public Records Act requests and litigation discovery. Users must follow section 3.2.3 to gain access to accounts belonging to other employees.

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.