# County of El Dorado

## Procedures and Guidelines

Information Technologies

*Version ~~3~~4.0*

*~~May~~July 202~~2~~3*

# *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. Examples of network resources include: workstations; data storage devices; peripheral devices (printers, scanners, etc.); servers; internet connections; mobile devices (laptops, tablets, smartphones); voice telephony devices; and any other electronic services accessed by Users in conducting their work.~~

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

~~**PHI (Personal 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.~~

**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 ~~anti-virus~~End-Point protection, and must meet all other technical specifications as determined by the IT Department following Computer & Network-Based Information Systems P~~p~~olicy 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 ~~Wednesday night~~ for mandatory weekly security updates. This includes assigned devices, shared devices, and devices in conference rooms. Users Teleworking need to follow guidelines in Telecommuting ~~p~~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.

~~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~~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, ~~all~~ data stored on the County information domain ~~must be retained and made~~ is considered discoverable. ~~This pertains to all data in the information domain, even if it is personal or 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 Department Heads, Human Resources, or County Counsel~~, or—in the case of Public Records Act requests—the Clerk of the Board~~.

### 3.2.1. Request for Own ~~Items~~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.
  - ~~o~~ 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.

~~**Note**:~~

~~All eDiscovery requests must be approved by either the department head, County Counsel, or Human Resources.~~

~~Supervisor (as defined in Active Directory) will have 60 days to review content in an employee's OneDrive and save content if needed after the account is deleted.~~

### 3.2.3. Request for Another Employee's ~~Items~~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 ~~, even if requested by the employee's supervisor, manager, or~~ must be approved by the employee's department head~~,~~ County Counsel, or Human Resources ~~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. ~~The methods and caveats are the same as listed for supervisor access above, with the exception the department head must approve the request.~~

~~Emails for "Active" Employees – Employees can delegate accounts in Outlook.~~

~~Emails for "Inactive" Employees – IT can delegate accounts for inactive employees. The department head must~~ay ~~request~~ IT create ~~the delegation. The IT standard is 30 days. Additional days can be requested with a justification.~~

~~OneDrive and H Drive for "Inactive" Employees -~~

- ~~The department head must~~ay ~~request~~ IT create ~~an eDiscovery case to review OneDrive items and H Drive within the County backup procedures. The case will remain open for 30 days.~~

## 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 credentials used by the County:~~

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 isSupport ticket for all employee transfers and employee terminations.

Each trusted external user (contractor, vendor, volunteers, outside agencies) shall ~~hall~~ have a uniquely assigned user ID to enable individual authentication and accountability. An External Trusted User form must be completed to define~~d~~ use and access level with authorization from the El Dorado County – department head prior to the user IDs ~~to~~ being issued. The Information Security Office (I~~O~~SO) 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.

- ~~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.~~

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)** ~~**Procedures**~~

All users (employees or ~~external~~ trusted external users) are required to engage in one additional

[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

authentication beyond username and password to access County resources when off network.

~~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.~~

#### ~~*3.3.2.1.* 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.~~
- ~~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 Information Security Officer (ISO) with any questions about password rules.~~

### 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 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

~~In some instances,~~ 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.

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

### ~~3.3.4.~~3.3.5. Protection of Credentials

Users are responsible for protecting ~~all of~~ 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. ~~***Do not EVER give***~~***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., ~~T~~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.

~~Users are encouragedy 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.)~~

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 ~~an~~ ~~is~~Support 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 ~~or~~and data protection guidelines.
- Users should understand when agreements need to be in place to share protected data ~~the~~ with departments and external users. Best practice is to use MS Teams to share with external users.
- Users are required to use sensitivity~~e~~ 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~~or~~ data protection guidelines.
- MS Team owners need understand when agreements need to be in place to share protected data ~~the~~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 ~~needs~~must to be approved by IT ~~using~~in alignment with Computer & Network-Based Information System P~~p~~olicy A-13.

### 3.4.4 Portable Data Storage Procedures

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

- The USB Drive~~needs~~must labeled, encrypted, and handled according to its data classification. ~~preferred~~

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

- Data transfers outside of controlled areas ~~are~~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 HIP~~P~~AA, set a standard for secure file transfer. Failure to comply with these standards can result in substantial penalties. Many ~~of these~~ 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.

- ~~Datan aA~~ Users need to have a data sharing agreement with external users on file when providing data ~~aremust be~~

- SFTP is a temporary storage. Users requesting SF~~P~~TP must provide a data retention timeline or IT will ~~place~~ automatically default to a 30-~~-~~day data retention~~policy~~ 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 ~~from the Internet~~ 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 ~~p~~ 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 C~~c~~ounty has licensed use or rights to the software or data.

~~"Fair Use" is a legal principle that allows the unlicensed use of copyright material under special circumstances. However, it is unlikely that County business needs will require invoking the Fair Use principle, so the use of photos or text from copyrighted sources in County documents (including PowerPoint slides) is strongly discouraged.~~ prohibited. 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.

~~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.~~

Employees should be aware that ~~on March 2, 2017, a decision by the California Supreme Court has made~~ 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

~~Users~~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.

~~ 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 on county issued devices~~, but will not be responsible for any changes, damages, or loss of data on personal devices that are used for remote access~~.

## 3.7. 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.~~ 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 ~~wifi~~Wi-Fi 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.

Users are not allowed to use County email accounts for personal use~~. This includes, but is not limited to, the creation of iTunes accounts on mobile devices.~~ , 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 ~~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~~ 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 ~~may not~~ to gain access ~~email~~ to accounts belonging to other employees.

~~Users are required to manage their own email~~access credentials~~, 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.~~.

# ~~Appendix A – Data Breach Response Procedure~~

## ~~1. PURPOSE~~

~~The purpose of the procedure is to establish the response process in instances where there is a potential or actual breach of privacy and confidentiality of protected information. This procedure will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The procedure shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.~~

~~El Dorado County Information Security's intentions for publishing a Data Breach Response Procedure are to focus significant attention on data security and data security breaches and how El Dorado County's established culture of openness, trust and integrity should respond to such activity to minimize the risk of any unintended disclosure. El Dorado County Information Security is committed to safeguarding personally identifiable and protected health information in the possession of the County, its employees, and contractors in accordance with federal and state laws and applicable regulatory requirements.~~

### ~~1.1. Background~~

~~This procedure mandates that any individual who suspects that a theft, breach or exposure of El Dorado County Protected data or El Dorado County Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Helpdesk@edcgov.us, by calling 530-621-5696, or through the use of the help desk reporting web page at http://helpdesk. This e-mail address, phone number, and web page are monitored by the El Dorado County's Chief Information Security Officer. The Chief Information Security Officer will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Chief Information Security Officer will follow the appropriate procedure in place.~~

## ~~2. SCOPE~~

~~This procedure applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Personally Identifiable Information (PII) or Protected Health Information (PHI) of El Dorado County constituents. Any agreements with vendors will contain language similar that protects the data.~~

## ~~3. PROCEDURE~~

### ~~3.1. Confirmed Theft, Data Breach or Exposure of El Dorado County Protected Data or El Dorado County Sensitive Data~~

~~As soon as a theft, data breach or exposure containing El Dorado County Protected data or El Dorado County Sensitive data is reported or identified, the process of removing all access to that resource will begin.~~

The Chief Information Security Officer will document the incident report and in collaboration with the Information Technology Director will chair an incident response team to coordinate the handling, investigation, and reporting of the breach or exposure.

The team will include members from:

- IT Infrastructure
- County Counsel
- Public Information Officer
- Risk Management
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved
- Additional individuals as deemed necessary by the Chief Information Security Officer

IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

## 3.2. Work with Forensic Investigators

As provided by El Dorado County cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

## 3.3. Develop a communication plan.

Work with El Dorado County Public Information Officer, County Counsel, Risk Management, and the affected departments for notification and communication of the breach to the appropriate individuals and/or agencies..

## 3.4. Ownership and Responsibilities

Roles & Responsibilities:

- Chief Information Security Officer is the employee of El Dorado County, supervised by the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant individuals.

- Users include virtually all members of the El Dorado County community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

- The Incident Response Team shall be chaired by the Chief Information Security Officer and shall include, but will not be limited to, the following departments or their representatives: IT- Infrastructure; Public Information Officer; County Counsel; Management; Risk Management.

### 3.5. Enforcement

Any El Dorado County personnel found in violation of this procedure may be subject to disciplinary action, up to and including termination of employment. Any third-party partner company found in violation may have their network connection terminated.

## 4. DEFINITIONS

**Breach –** acquisition, access, us, or disclosure of Protected data and Sensitive data in a manner that is not permitted under applicable laws and regulations.

**Protected Health Information (PHI)** - information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

**Personally Identifiable Information (PII)** - Any data or information that could be used alone or when combined with other sources to uniquely identify, contact, or locate a specific individual. Examples of PII include, but are not limited to: name, social security number, biometric records, date and place of birth, mother's maiden name, etc. Protected data - See PII and PHI

**Information Resource** - The data and information assets of an organization, department or unit.

**Safeguards** - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

**Sensitive data** - Data that contains PII or PHI data. See PII and PHI above.