BOARD OF SUPERVISORS, COUNTY OF SIERRA, STATE OF CALIFORNIA

RESOLUTION UPDATING THE SIERRA COUNTY INFORMATION TECHNOLOGY (IT) POLICY

Resolution 2023-074

WHEREAS, the Board of Supervisors previously adopted an Electronic Media and Use Policy/Information Technology Policy pursuant to resolutions 2009-067, 2016-034, 2017-117, 2020-011, and 2023-065 which policy governs the appropriate uses, processes, and procedures by which county employees shall use the County's electronic media and devices, and

WHEREAS, electronic media and devices are a topic of constantly evolving practical, technical and legal requirements and best practices which requires continual review and updating, and

WHEREAS, the attached updated Information Technology Policy has been reviewed and edited by staff.

NOW, THEREFORE, BE IT RESOLVED that the Sierra County Board of Supervisors, County of Sierra, State of California does the attached Information Technology Policy, dated June 2023, is hereby adopted by the County Sierra. This Policy shall supersede any prior County policy on the same subject matter.

ADOPTED by the Board of Supervisors of the County of Sierra on the 20th day of June, 2023, by the following vote:

AYES:
NOES:
ABSTAIN:
ABSENT:

COUNTY OF SIERRA

SHARON DRYDEN, CHAIR
BOARD OF SUPERVISORS

ATTEST:

HEATHER FOSTER
CLERK TO THE BOARD

APPROVED AS TO FORM:

DAVID PRENTICE
COUNTY COUNSEL

Sierra County

Information Technology Policy

June, 2023

Table of Contents

Purpose 2

General 2

1. **Employee-Owned Equipment** 3
2. **Electronic Communications** 3
3. **Login Credentials** 4
4. **Software** 4
5. **Data Integrity** 4
6. **Incidental Personal Use** 4
7. **Casual Remote Access** 5
8. **Remote Access/VPN (Virtual Private Network) Policy** 5
9. **Privacy Limits** 7
10. **Public Records Act Litigation** 7
11. **Confidentiality** 8
12. **Restrictions** 8
13. **Inappropriate Use** 8
14. **Attorney-Client Privilege** 9
15. **Discipline** 10
16. **Document Retention** 10
17. **Mobile Data Device Policy** 10

COUNTY OF SIERRA

Information Technology Policy

Purpose

Information and the systems, networks, and software necessary for processing are essential Sierra County assets that must be appropriately protected against all forms of unauthorized access, use, disclosure or modification, Security and controls for County information and associated assets (County IS Assets) must be implemented to help ensure privacy, confidentiality, data integrity, availability, accountability, and appropriate use. This policy establishes the minimum standard to which all departments must adhere. Departments may, with the approval of the Information Systems Department (IS Department), enhance the minimum standard based on their unique requirements. This policy governs all Electronic Communications Resources including, but not limited to, the Internet, E-mail, voice-mail, cellular telephones, pagers, personal digital assistants, smartphones, Blackberry devices, computers/laptops, telecommunications devices, video and audio equipment, wireless networks, data systems telecommunications equipment, transmission devices, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, software, County-related social media, and documentation that supports electronic communications services ("Electronic Communications Resources").

General

The County of Sierra encourages the use of electronic communications resources to share information in support of its mission of public service and to conduct its business. The County owns and operates a variety of computers, network, electronic mail (hereinafter "e-mail"), Internet access and voice communication systems for use by its employees. These systems are provided to employees at the County's expense to assist the employees in carrying out the business of the County.

Social media tools and websites such as Twitter, Facebook, LinkedIn as well as services such as Instant Messaging/Chat, Comments, Wikis, Blogs, Groups, Skype, and VoIP are similar to e-mail as communication methods and for the purpose of this policy, are equivalent in all aspects to e-mail. As such, social media services/tools/technologies including instant messaging are inclusive to all references to e-mail in this policy.

Department use of social media technology must conform to the policies, protocols and procedures contained, or referenced, herein.

Social media applications used by Departments must be approved by the Board of Supervisors prior to use.

Employees are not guaranteed access to County-owned devices or networks, and are not guaranteed permission to use personal devices for County business. Remote access is not guaranteed and requires pre-approval.

1. Employee-Owned Equipment

Employee privately owned equipment (cell/smart-phones, note/net-books, tablets, computers and other current and future devices) shall not be authorized to be used to conduct County business. The Board of Supervisors, Department Managers and Department Mid-Managers are authorized to use personal devices to conduct County business.

The Board of Supervisors, Department Managers and Department Mid-Managers should be aware that privately owned equipment may, as part of litigation or other legal processes, be subject to seizure for review of the county owned data and therefore, the County requires that all employees not authorized in this policy use county-owned equipment for conducting County business.

Employees are allowed to use their personal cell phones as the authenticating device to validate their Multi-Factor Authentication to County logins should they choose. This use does not subject the employees' personal phone to the same level of security and access control required when using the device for County business nor does it subject the employees phone to a PRA (Public Records Act). Therefore, County IT has no need to have the ability to wipe any data from that device.

Should the County need to review an employee's privately owned equipment for county purposes, the County will comply with all state and federal laws and regulations regarding employer access to employee-owned equipment.

2. Electronic Communications

The County's email system is the official communication tool for County business. An official email address is established and assigned by the County to each employee. All County communications sent via email will be sent to this address. County employees must use the official County email, instead of their private email address (such as Yahoo, Google, Hotmail, etc.) when communicating County business via email. Electronic Communications Resources must be used in compliance with applicable statutes, regulations, and County's policies including those that require a work environment free from discrimination and harassment. Electronic communications should conform to the same standards of propriety and respect as any other verbal or written communication at the County. Employees are expected to use common sense and judgment to avoid any communication which is disrespectful, offensive, or illegal.

The County, as the provider of access to its Electronic Communications Resources, reserves the right to specify how those resources will be used and administered to comply with this policy. It is important to realize that the message content sent from the County's account reflects upon the County (positively or negatively) to those who receive the message. Electronic communications to recipients on systems outside of County pass through systems and networks not managed by the County. The privacy and confidentiality of these messages is, therefore, not assured. In addition, some delivery methods and networks impose legal restrictions regarding the nature of messages allowed. Users are expected to comply with all such regulations. Employees and other users of the Electronic Communications Resources may create criminal and civil liability for themselves and the County by using outside or third-

party systems in an offensive, defamatory or illegal manner and in such event employees and other users may be subject to disciplinary action up to and including termination.

It is the County's responsibility to ensure availability of a device for the employee to be able to access this account. It is the employee's responsibility to check the account for county communications on a regular and frequent basis.

3. Login Credentials

Employees are required to keep their assigned personal login credentials that include username and password, private and safe and not share it with anyone. This password will be required to meet complexity requirements put in place by the Information Systems Department and will be reset annually unless stricter requirements are required.

4. Software

Only software that has been purchased or authorized by the County of Sierra Information Systems Department may be installed onto County owned computers or other communication equipment including cell phones. All software vendors must complete a Vendor Application Information Questionnaire and return it to the Information Systems Department for approval prior to commitment of purchase. To assure that all software is licensed and virus free, all software that is to reside on the LAN or personal computer disk drives will be installed by the Information Systems Department. All software or data brought in from outside the County (whether via physical media or via download) must be scanned by an updated County approved anti-virus and anti-malware software program before being loaded onto any County computer system. Downloading programs from outside sources such as the Internet must be pre-approved by Information Systems Department. All such programs will be scanned for viruses and malware. Such programs will be necessary and related to County business.

All equipment connected to the County of Sierra network must be authorized by the Information Systems Department prior to attaching to the network or associated peripherals. At no time should any employee plug a device into the ethernet ports on the network. This includes Smart TV's. Those County owned devices must be added to the Counties Sierra-IOT secured network by the Information Systems Department.

5. Data Integrity

Users are responsible for maintaining the integrity of County data. Users may not knowingly or through negligence cause County data to be modified or corrupted or accessed in any way that compromises its accuracy or prevents authorized access.

6. Incidental Personal Use

Electronic Communication Resources are provided by the County to facilitate the performance of County work. Under no circumstance other than that which is expressly permitted, should an employee use any County resource for personal use. Incidental personal use is permitted for reasons of personal necessity so long as employee use of the systems are made during the time the employee is relieved from duty (i.e. during a break, during the employee's lunch hour, or before or after the employee's work shift), and

only so long as the Department Head determines that the operation of the Department is not being compromised or disrupted.

Incidental personal use should be minimal, and should not:

- interfere with the County's operation of Electronic Communications Resources;
- interfere with the user's employment or other obligations to the County, or
- burden the County with noticeable incremental costs. Incidental use of the County's Electronic Communications Resources should clearly indicate that the use is personal.

Users of Electronic Communications Resources shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the County unless appropriately authorized to do so. The County is not responsible for any loss or damage incurred by an individual as a result of personal use of the County's Electronic Communications Resources.

7. Casual Remote Access

Modern business practices often provide for an employee to be able to check electronic communications tools from home or other non-work sites, which will be referred to as "Casual Remote Access". Communication tools are voice mail, email, electronic calendar, or other similar tools. Casual Remote Access does not qualify for over-time compensation as Casual Remote Access is voluntary and not at the direction of management, however, this privilege may be removed at the direction of the Department Manager. Non-Manager employees must access online resources through the web portal on the Sierra County website. The purpose of this access is not to conduct county business but to allow employees an opportunity to stay connected to communications when away from the office.

- This section is intended to facilitate casual remote access, when appropriate, and to define the restrictions and responsibilities of employees and others who are authorized casual remote access. Managers and other employees, who are not subject to overtime pay, may have fewer limitations to casual remote access than other employees. Contractors, consultants, non-County agencies, and others who are authorized to use the County's computer networks, may be subject to these provisions.

- The County's Email System can be accessed from non-work locations through a specific secure website via a web browser or other electronic communications tools. The Department Head, or his/her designee, will establish the appropriate restrictions for the employee's casual remote access to e-mail. In some situations, the department may expect an employee who is out of the area at a work-related training or conference to check email, similar to expectations to check and respond to voice mail as part of the normal workday. In some situations, during non-work time an employee may be authorized, for their own convenience and in a non-pay status, to access e-mail, voice mail, or their schedule for minimal amounts of time. The department has flexibility to authorize an employee to work or work overtime, via casual remote access; however, this policy is not intended to replace the County's Telecommuting Policy.

- The process for accessing the County's email or other electronic tools has been set up by the Information Systems Department, who reserves the right to discontinue the service if the need arises.

8. Remote Access/VPN (Virtual Private Network) Policy

This section contains the standards for connecting to Sierra County's network from a remote location. These standards are designed to minimize the potential liability exposure to the County, which may result from unauthorized use of County resources, such as the loss of sensitive or confidential data, violation of intellectual property, damage to the County's public image, damage to critical County internal systems or damage to third-party or County property.

This policy applies to all employees, volunteers, contractors, consultants, non-County agencies, and others who are authorized to access the computer networks. This policy applies to remote access connections used to do work on behalf of Sierra County, including reading or sending email and viewing intranet web resources.

- The following definitions are used in this section:

  A. VPN - Virtual Private Network - a means of connecting a remote computer to a network across the Internet by creating a secure encrypted tunnel.

  B. DMZ - Demilitarized Zone - a network segment on a Firewall that is outside the internal network (lower security) and inside the Internet (higher security), used for placing devices that may need to be accessed by the Internet (Web servers, etc.).

  C. Remote Access - a means of accessing core network resources from a site not physically connected, accomplished by Dialup connection, or a DSL, or Cable modem, with a VPN tunnel.

- The following are the limitations on remote access:

  A. VPN access is permitted to County employees only and only with authorization.

  B. No employee will be provided with VPN access without specific written consent from their Department Head and the Information Systems Department.

  C. Remote access will be granted for authorized County work only. All remote access to the County network will be accomplished via Palo Alto Global Protect, a secure remote access method (including, but not limited to, strong authentication, Virtual Private Network (VPN), controlled dial-in/dial-out, firewall demilitarized zone (DMZ)).

  E. Access from a remote site to a County network that contains sensitive or restricted information may require extended identification and authentication procedures as well as additional authorization.

  F. Access to County resources will only be allowed from County owned and controlled computers, unless otherwise authorized by the Information Systems Department. All authorized employees accessing the County network from their privately-owned computers will exercise due diligence in ensuring that their systems (both hardware and software) are free from computer viral and malware infection, precluded unauthorized use, including unauthorized use by non-County employees, or by County employees who have not been specifically authorized for such access.

G. When an authorized user terminates employment or transfers to another department or office, all existing remote access services will be terminated. Remote access will have to be re-justified and re-established for any new County position. County owned hardware must be returned and software permanently deleted from privately-owned equipment.

H. VPN Access must be renewed and authorized annually.

Department Heads are responsible for contacting the Information Systems Department to receive/complete/file the Virtual Private Network Use Agreement.

Once the required Agreement has been filed with the Information Systems Department, the Information Systems Department will provide the authorized employee virtual access to the network. If the requesting department does not have a County-owned and County-monitored computer available, the Department will contact the Information Systems Department to determine if one is available elsewhere. Departments that have County-owned and County-monitored computers must ensure those computers are plugged into the County network weekly to receive security and software upgrades.

9. Privacy Limits

Users of County e-mail and communication systems should be aware that:

(1) their e-mail/communications are not personal and private;

(2) their email/communications may be (but are not necessarily) saved for future reference; and

(3) their email/communications may be seen by persons other than the original addressee.

Subject to the restriction regarding obtaining County Counsel's permission under certain circumstances, the County of Sierra reserves the right to monitor or review e-mail messages and any information stored or transmitted on its equipment without advance notice to the users thereof. All such communications are the property of the County of Sierra and may be accessed. The County reserves the right to specify how the County's network resources will be used and administered to comply with this policy and all documents. Other than those going to, or from, or within County Counsel's Office, designation upon such communications (e.g. "personal", "private" or "confidential") will not result in the document receiving any greater degree of privacy or confidentiality than that which would normally be given such communication and no employee should have an expectation of privacy in any message or communication he or she creates, receives, stores, sends, or deletes from any of the systems.

Employees should not communicate their private, privileged, or confidential information, including but not limited to personal attorney client communications, financial or medical information and other privileged information, via the County's Electronic Communications Resources. Employees who do communicate their private, privileged, or confidential information via the County's Electronic Communications Resources will be deemed to have waived any privilege or privacy rights in those communications, even where those communications are made via personal password protected accounts using the County's Electronic Communications Resources.

Additionally, the County may be required to produce information transmitted or stored on its Electronic Communications Resources pursuant to a court order, subpoena, or statute.

10. Public Records Act and Litigation

The California Public Records Act requires the County to disclose specified public records. In response to requests for such disclosure, it may be necessary to examine electronic communications records that users may consider to be personal to determine whether they are public records that are subject to disclosure.

All communications transmitted via the County's Electronic Communications Resources, whether or not related to personal or confidential matters, are subject to monitoring, at the County's discretion. Communications under these systems may also be discoverable during the course of legal proceedings. Nothing in this policy will be construed to allow disclosure to the public under the Public Records Act or discovery production in a civil lawsuit of otherwise privileged or confidential information. An employee will consult with his/her department head regarding department policy before sending information subject to state and federal privacy laws (e.g., Health Insurance Portability and Accountability Act, "HIPAA").

For further information, please refer to the County of Sierra Public Records Act Policy for Private Devices and Accounts dated September, 2017.

11. Confidentiality

California law requires that certain information be treated as confidential and not be distributed to others inside or outside the County who do not have authorization to view such information. Some examples of confidential information are personnel records, medical records, internal investigations, on-going civil and criminal investigations, criminal records, information relating to litigation or potential litigation, attorney-client communications, information relating to labor negotiations, or information relating to confidential real estate negotiations. Confidential information should not be sent, forwarded, or accessed by individuals or entities not authorized to receive that information and should not be sent, forwarded, or accessed by County employees not authorized to view such information. Employees shall exercise caution in sending confidential memoranda, letters, or phone calls, because of the ease with which such information can lose confidentiality by inadvertent or intentional diversion or re-transmission by others.

Employees who access, via his/her device, Protected Health Information (PHI), and/or Personally Identifiable Information (PII), and/or any other data deemed by policy or statute to require encryption, are required to maintain the settings on his/her device such that data encryption is enabled at all times.

12. Restrictions

The information sources accessible via the Internet are worldwide and constantly growing in kind and number. It is not possible for any Internet access provider to fully manage the types of information accessible by its systems and users, especially with regard to content limitations. Nonetheless, the County reserves the right to restrict access to any data source, at its sole discretion. These restrictions do not constitute an implication of approval of other non-restricted sources.

13. Inappropriate Use

Without exhausting all the possibilities, the following are examples of inappropriate use of the County's Electronic Communications Resources and County telephone, cell phone and voice mail systems:

- Creating, viewing, accessing, downloading, storing, or exposing others unwillingly, either through carelessness or intention, to material which is offensive, obscene or in poor taste. This includes information which could create an intimidating, offensive or hostile work environment.
- Any use that may, for a reasonable person, create or further a hostile attitude or give offense on the basis of race, color, religion, national origin, citizenship, ancestry, marital status, gender, disability, age, veteran's status or sexual orientation;
- Communicating confidential County or HIPAA classified information to unauthorized individuals within or outside of County;
- Sending messages or information which is in conflict with applicable law or County policies, rules or procedures;
- Attempting to access unauthorized data or break into any County or non-County system;
- Engaging in theft or the unauthorized copying of electronic files or data;
- Performing acts that are wasteful of computing resources or that unfairly monopolize resources to the exclusion of others is prohibited. These acts include, but are not limited to sending mass mailings or chain letters and creating unnecessary network traffic;
- Intentionally misrepresenting one's identity for improper or illegal acts;
- Engaging in unlawful activities;
- Engaging in commercial activity or activity for financial gain, not under the auspices of the County;
- Engaging in recreational use of the County's Electronic Communications Resources that interferes with the ability of the employee or other users to conduct County work. This includes but is not limited to downloading or uploading software, games, or shareware. Employees are also prohibited from downloading and using instant messenger (IM) for recreational use;
- Advertising or soliciting for commercial ventures, personal business, or to perform an illegal or malicious act; and
- Illegal copying of computer software protected by copyright.

If an employee receives an unreasonable amount of personal email or email that is inappropriate as described above, the employee is required to immediately give notice to the sender(s) of the email to cease further issuance of the subject emails. Knowledge of passwords, loopholes, or other means of gaining access to network, data, communication, application, server, document, website, device, and associated computer security systems will not be used to damage computing information or resources, obtain extra information or resources, take information or resources from another user, gain unauthorized access to information and resources, or otherwise make use of information or resources for which proper authorization has not been given.

Accessing data on the County computer systems unless expressly authorized is strictly prohibited.

14. Attorney-Client Privilege

In order to preserve the attorney-client and attorney work-product privileges, e-mail communication to, from, or within County Counsel's office may not be opened, except by a person to whom it was properly addressed or with County Counsel's express permission. Employees who send an e-mail containing confidential information to County Counsel should be aware that the confidential nature of such e-mails is subject to challenge in the courts and that preservation of these privileges requires limiting disclosure of the e-mail to essential recipients only. These limitations on monitoring do not apply to incoming or outgoing Internet e-mail for automated virus and spam protection, or Intrusion Detection Systems, nor do these limitations apply to monitoring by Sierra County Information Systems Department either externally or internally for Security or Quality of Service purposes as long as such e-mail are not opened and read by a person who has not received the County Counsel's permission.

15. Discipline

Employees may be subject to disciplinary action for using the Electronic Communications Resources in a manner other than for their intended purposes, or in a manner that violates applicable laws, rules, and policies. Any violation of this policy will be considered grounds for disciplinary action up to and including termination, and/or civil and/or criminal prosecution under County, State, or Federal laws.

16. Document Retention

Electronic files, documents, and e-mail messages should be treated the same as paper documents with regard to the laws pertaining to a public entity's retention and destruction of documents and records (Government Code Section 26200, et seq.). Accordingly, employees and elected officers may have an obligation to retain certain documents and e-mail communications for a specified period of time. Employees should seek the advice of their Department Heads in order to ascertain the specific time requirements, which apply to the documents generated, received, and/or maintained by their departments. An e-mail communication will be deleted from the email system after 60 days or as soon as practicable from the electronic communications system by an elected officer or an employee (recipient and the sender) without preserving the informational content of such communication, or any portion thereof, in archival form unless: 1) a law expressly requires such communication to be kept; 2) preservation of such communication is necessary or convenient to the discharge of the elected officer's or the employee's duties and such communication was made or retained for the purpose of preserving its informational content for future County use or reference; 3) in the event a public inspection request is made pursuant to the Public Records Act, or a demand by subpoena or court order is received by the County, for any communication in existence at the time such request or demand is received, or 4) whenever the potential for litigation arises, or has arisen, with respect to the matter communicated in the e-mail. For purposes of this section, retention of e-mails falling into the four specified categories will be accomplished by either saving the communication on the elected officer's or the employee's user account by archiving the file to portable document format (.pdf) or by printing a hard copy of the communication on a printer and depositing it in a folder named "archives".

An e-mail saved in this manner may be destroyed pursuant to Government Code §26202 when it becomes more than two (2) years old. In addition, each department may have set a destruction of records schedule for various types of records. An e-mail falling into a category that is to be kept longer

than two (2) years will be printed and the hard copy placed in the appropriate category's file for retention beyond the two (2) year period hereby established for e-mails in general.

17. Mobile Data Device Policy

Mobile electronic communication devices can connect to the County network for the purpose of synchronizing data contained in an employee's County Microsoft 365 user account. Because of the mobility and the size of these devices, they are susceptible to being misplaced, lost, or stolen; therefore, protecting the information contained on these devices from being viewed and/or exploited by unauthorized personnel is of the utmost importance.

Employees and elected officials whose job duties require them to use a cell phone for official County business to maintain communication abilities including, in some cases, holidays, weekends and other non-regular work hours, may receive County-provided phones.

(1) An employee's job duties must meet at least one of the following criteria to be considered for a cell phone allowance:

(a) The job requires considerable time outside the office (travel, meetings, conferences, etc.) and use of an electronic device facilitates the effective maintenance of business operations while away.

(b) The job requires the employee to be immediately accessible to receive, respond to and/or make frequent business calls and/or emails outside normal working hours and/or the office environment.

(c) Job duties away from the office may expose the employee or others to immediate harm or danger (e.g., visits to homes of patients or clients).

These positions will be determined by the Department manager or his/her designee.

Personal Device for County Business Use: The Board of Supervisors, Department Managers, and Department Mid-Managers on salary, shall be afforded the opportunity to use a personal device to utilize for County business if it is able to meet the County's data protection guidelines and an acceptable use policy is signed allowing the county to protect the data on the personal device. The Board of Supervisors, Department Managers, and Department Mid-Managers are required to have or maintain a cellular mobile device, whether owned personally or provided by the County. Other employees will be assigned a County maintained device at the discretion of the Department Manager. These devices shall not be allowed to be used for personal use. Mobile devices are required and expected to be always powered on and accessible to the employee during working hours. All mobile device phone numbers used for County business, whether they are personal or county-owned, will be published in the employee directory. Mobile devices will be required to be relinquished immediately upon request of the Information Systems Department or Department Manager.

1) Mobile Data Device

A. This section defines the proper use of mobile electronic communication devices connected to the County network as well as important safeguards that must be followed.

B. The purpose of this section is to establish standards for the use of mobile electronic communication devices connected to the County network. These standards are designed to prevent unauthorized access of County information.

2) The following definitions are used in this section:

A. "Mobile Data Device" – a computing device that is usually much smaller than a typical laptop computer that is easily transported from place to place. These devices communicate with various networks using one or more wireless technologies - usually Wi-Fi and/or a cellular phone network. These devices are distinguished from desktop and laptop computers by the fact that a mobile data device cannot be joined to the County network through a standard Active directory configuration. Some examples of mobile data devices are smartphones, tablets, and other devices running a mobile operating system.

B. "Smartphone" – a mobile telephone that also includes many of the features of a standard computer. Some of the features might include sending/receiving email, browsing the Internet, and loading software applications (apps). Some common smartphones are Blackberry, iPhone, and phones using the Android operating system.

C. "Personal Mobile Data Device" – a mobile data device that is owned by the employee and where, if the device can communicate via a cellular network, the employee is personally responsible for all charges that are incurred through the cellular network carrier.

D. "County Provided Mobile Data Device" – a mobile data device that is provided by the County and where, if the device can communicate via a cellular network, monthly charges incurred through the cellular network carrier are paid for by the County.

E. "Secure Digital (SD) Cards, Compact Flash (CF) Cards, Memory Sticks, Flash-Based Supplemental Storage Media" – different types of memory that can be added to increase the storage capacity of some mobile data devices.

F. "KILL" – This is the term used to describe the process of removing a mobile data device's connection to the County network. This process includes blocking County user accounts from logging into the device as well as removing all County Data from the Mobile Data Device.

3) When a department is contemplating issuing a County provided mobile data device, they may coordinate with the Information Systems Department to identify device specifications and functionality requirements. Sierra County will only provide Approved Cell Phones with the Android Operating System.

4) For personally owned devices, the privilege of having a smartphone connected to the SierraMobile WiFi on the County network requires the employee to comply with certain responsibilities and rules pertaining to the use and security of data contained on the smartphone.

A. Failure to comply with these responsibilities and rules will result in immediate suspension of the employee's connection to the County network.
B. Depending on the severity of the offense, the employee may face further discipline.
C. The Chief Technology Officer, or his/her designee, will make the final determination as to whether a mobile data device will be connected and/or remain connected to the County network.

5) It is the responsibility of the employee who is connecting to the County network to ensure that all components of his/her connection remain as secure as his/her network access within the County. It is imperative that any wired or wireless connection, including, but not limited to mobile data devices and service, used to conduct County business be utilized appropriately, responsibly, and ethically. The following rules must be observed by employees that are using a mobile data device connected to the County network:

A. The types of devices that are allowed to connect to the County network are limited. Consult with the Sierra County Information Systems Department (County IT) to determine the current devices and software versions that are supported. Devices connecting to Sierra_Mobile may require the installation of the Counties End-Point Protection Software, Palo Alto Cortex as well as the device may need to be added to Microsoft InTune Mobile Device Management software. No cell phone, County assigned or personal, shall be used to access the SierraPrivate wireless network without consulting with the CTO or his/her designee.

B. Some mobile data devices may require the purchase of a software application (app) or license to allow the mobile data device to comply with County IT mandated security requirements.

1. Personal Mobile Data Device - Employee is responsible for all costs of required software applications. If the mobile data device can communicate with a cellular network, it is the employee's responsibility to set up his/her individual calling plan with their cellular network provider and to pay all charges incurred.
2. County Provided Mobile Data Device - With the employee's Department Manager, or his/her designee, approval, the department will purchase the required software application.
    a. If software applications are required, the department requesting connection of the County provided device will be responsible for making this purchase prior to the device being connected to the County network.
    b. The employees' department is responsible for all costs of required software applications.

C. Employees who access, via their mobile data device, Protected Health Information (PHI), and/or Personally Identifiable Information (PII), and/or any other data deemed by policy or statute to require encryption, are required to maintain the settings on their mobile data device such that data encryption is enabled at all times.

D. Privacy

1. Personal Mobile Data Device - By voluntarily connecting a personal device to County resources, employees shall not have any reasonable expectation of privacy concerning all information stored or network traffic on his/her device. While it is not the intention of the County to review what personal device is being used for; it should be expected that in protecting the Sierra County's data networks, it is the responsibility of the Information Systems Department to monitor suspicious activity and data traffic on the network, and in rare and limited cases, information stored on the personal device, or data in traffic to the personal device, may be exposed to IS Staff on the County's network.

The County reserves the right to review and access at any time all information stored on personal devices, including, but not limited to, wireless devices, which are used to connect to County resources, such as email. Employee access and/or connection to the County network may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity to identify accounts or systems that may have been compromised by external parties. When an employee voluntarily connects a personal device to County resources, the County has the right and

the ability to review and access any and all information on the employee's personal device, including data the employee may view as personal. The County's right and ability to review and access any and all information on that personal device exists for the entire time the employee uses the device to connect to County resources. Should an employee wish to terminate the connection to County resources, employee shall submit the personal device for access and review by County IT to ensure that all County related information is removed from the personal device. Any employee who refuses to surrender a personal device connected to County resources when requested by his or her supervisor to access and review the information on the device may be subject to disciplinary action. The County agrees it will not seek access to a Personal Mobile Data Device without notifying the employee of the County-related reason for the demand for access. The County does not have any intention of seeking access to an employee's Personal Mobile Data Device for reasons other than those which affect the County or the employee's working relationship with the County.

2. County Provided Mobile Data Device - Employees shall have no reasonable expectation of privacy concerning any and all of the information stored on a County provided device. The County reserves the right to review and access at any time all the information stored on county provided devices, including, but not limited to, wireless devices, which are used to connect to County resources, such as email. Employee access and/or connection to the County network may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity in order to identify accounts or systems that may have been compromised by external parties. When an employee voluntarily accepts a County provided device, the County has the right and the ability to review and access all information on that device, including data the employee may view as personal. Should an employee wish to stop using a County provided device, the employee shall return the County provided device. Any employee who refuses to surrender a County provided device when requested by his or her supervisor shall be subject to disciplinary action up to and including termination.

E. Employees accessing any County network with Mobile Data Devices, are required to know and adhere to all County policies and guidelines, including policies and procedures concerning the confidentiality of the data being accessed and personal activities during work hours.

F. Any and all data obtained via the County network remains the property of the County in perpetuity.

G. Passwords and other confidential data are not to be stored on any associated storage devices such as Secure Digital (SD) and Compact Flash (CF) cards, as well as Memory Sticks and related flash-based supplemental storage media.

H. Employees who dispose of their personal device or return it to the vendor must remove all County information from the device before disposing of it or returning it to the vendor. Employees can contact County IT if they need assistance in removing County information from the employee's device.

I. Employees must immediately report a missing, replaced, or stolen Mobile Data Device to County IT and to their personal cell carrier if applicable. County IT will send a "KILL" command that will clear County data from the device.

J. For Personal Mobile Data Devices and for County Provide Mobile Data Devices where the department permits the employee to store personal data on the Mobile Data Device, it is the employee's responsibility to back up their personal data, settings, media, or applications in the event the device has to be "KILLED" by County IT.

K. The mobile data device is subject to a remote "KILL" under the following conditions:

- Lost or stolen device
- Ten consecutive failed password attempts (assumes the device is no longer in the owner's possession)
- Employee leaves the employment of the County
- Department Head, or his/her designee, request
- County IT determines that any access to the County network is at risk (subject to approval of the Chief Technology Officer, or his/her designee)

L. Employees must abide by all municipal, state, and federal laws concerning the use of mobile devices.

M. All Mobile Data Devices connected to the County network will be required to comply with complex password policies and basic security restrictions. This means that to use the device, the employee will have to unlock the device by the approved methods.

1) Encryption
    (a) Required
2) Maximum minutes of inactivity until screen locks
    (a) 5 Minutes
3) Number of sign-in failures before wiping device
    (a) 10
4) Password
    (a) Required
5) Password complexity
    (a) Medium
6) Password expiration (days)
    (a) 365
7) Required password type
    (a) At least alphanumeric with symbols
    (b) Fingerprint Biometrics

**While stricter security settings are always recommended, the above list will provide a baseline level of protection against unauthorized access to County data.

N. All Mobile Devices must be accessible by County IT via pin code. If pin is changed, information Systems must be notified immediately.

O. County IT will charge the employees' department the current IT Professional Service hourly rate for all support of personal devices connected to the County. The employee must follow his/her department's procedures for obtaining services from County IT.