PLUMAS COUNTY ACCEPTABLE USE POLICY

Adopted by the Plumas County Board of
Supervisors December 6, 2022

COUNTY OF PLUMAS

ACCEPTABLE USE POLICY

Contents

I. Purpose:

The purpose of this policy is to describe the acceptable use of Plumas County's technology assets (e.g., hardware, software, data, and authentication information) by County employees, and occasionally others such as contractors and volunteers (collectively referred to in this policy as "employees"). Acceptable use of technology assets is essential to ensure Plumas County meets its regulatory requirements and maintains the confidentiality, integrity, and availability of technology assets used to provide public services.

This policy establishes the acceptable usage guidelines for all Plumas County-owned technology resources. These resources can include, but are not limited to, the following equipment:

- Computers
    - Desktop Computers, Laptops, Mobile Devices, Servers, etc.
- Network Equipment
    - Switches, Routers, Network, and Communications Cabling, Wall Plates, Wireless Antennas, Wireless Bridge Devices, Fiber Optic Lines, Fiber Optic Equipment, VoIP Phones, etc.
- Audio/Video Equipment
    - Video Codecs, HDTVs, Document Cameras, Projectors, Security Cameras, Miscellaneous Cabling, Digital Cameras and Camcorders, Printers, Copiers, Fax Machines, etc.
- Software
    - Operating Systems, Application Software, etc.
- Resources
    - Group Drive File Storage, Website File Storage, Email Accounts, Social Networking Accounts, etc.

This policy applies to all employees, contractors, consultants, temporaries, and other workers at Plumas County, including all personnel affiliated with third parties, including vendors. This policy also applies to all equipment that is owned or leased by Plumas County.

II. Overview

While Plumas County's IT Department (PCIT) desires to provide a reasonable level of freedom and privacy, users should be aware that all Plumas County-owned equipment, network infrastructure, and software applications are the property of Plumas County and therefore are to be used for official use only. Also, all data residing on Plumas County-owned equipment is the property of Plumas County and therefore, should be treated as such, and protected from unauthorized access.

The following activities provide a general roadmap to using Plumas County's technology resources acceptably:

- All passwords used to access Plumas County systems must be kept secure and protected from unauthorized use.
- No user account can be shared between individuals. Authorized users are responsible for the security of their passwords and accounts.
- Do not transfer personally identifiable information on portable equipment and storage devices.
- Do not keep personal data on your county devices (computer, laptop, etc.).
- All computers residing on the internal Plumas County network, whether owned by the employee or Plumas County, shall be continually executing approved virus-scanning software with a current, up-to-date virus database.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders.

- Personally identifiable information (PII) cannot be sent via electronic means unless through an encrypted email. PII should be transferred within the internal network, via an encrypted email, or through secure Virtual Private Network (VPN) connections.
- Off-campus work should be completed via a secure VPN connection so that no data is transferred off-network.
- All workstations should be kept secure. Users should lock the workstation when not attended to protect unauthorized users from accessing secure files.
- Under no circumstances is an employee of Plumas County authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Plumas County-owned resources.

III. Exceptions

Requests for exceptions to this policy must follow the PCIT information security policy exceptions handling process. Please open a ticket with the helpdesk to request a policy exception.

IV. Definitions

All definitions are contained within the Acceptable Use Policy and Standards Glossary.

V. Policies

Acceptable Use Behavior

Plumas County must protect the confidentiality (authorized access to systems and information), integrity (authorized modification of systems and information), and availability (making sure systems and information are available when needed) of all technology assets supporting Plumas County’s services. When engaged in the performance of your role with Plumas County:

- Attempts to disable or circumvent any Plumas County security controls, policies, or procedures (e.g., disabling virus protection or installing unauthorized software) are prohibited. This includes, but is not limited to:
  - Use of tools that compromise security (e.g., password crackers, network sniffers, attack frameworks and software distributions, proxies, unauthorized VPN clients, or other tunneling technology), except as authorized by the Plumas County Information Technology Director.
  - Attempts to disable, defeat, or circumvent any Plumas County information security components.
  - Intentional or careless interference with the normal operation of Plumas County technology assets.
- Use that violates Plumas County policy or local, state, and/or federal laws is strictly prohibited. This includes, but is not limited to:
  - Theft of Plumas County technology assets, including sensitive data.
  - Use of Plumas County systems for any type of harassment, which includes using any words or phrases that may be construed as derogatory based on race, color, sex, age, creed, disability, marital status, national origin, religion, pregnancy, gender, gender identity or expression, genetic information, sexual orientation, veteran or military status, use of a service animal, or any other status protected by federal, state and local law.
- Unauthorized use, destruction, modification, or distribution of Plumas County external and internal systems, applications, and data is prohibited. This includes, but is not limited to:
  - Release or disclosure of Plumas County data to unauthorized parties inconsistent with federal, state, and local law (e.g., HIPAA, Chapter 42.56 RCW), Plumas County policies, or inconsistent with your assigned job role and responsibilities.

- Attempts to modify administrative settings and configurations or repair hardware and software. Such modifications, configurations, and repairs shall only be performed by authorized technology support personnel for your department or agency. This excludes basic troubleshooting such as closing and restarting an application or a restart/reboot of a single workstation. Modification, configuration, and repairs of enterprise information technology equipment and networking infrastructure shall only be performed by authorized support personnel in PCIT.
- Removal of technology assets from Plumas County premises without prior approval by authorized technology support personnel for your department or agency is prohibited. This excludes technology issued directly to you for employment purposes approved for taking home or from Plumas County premises by your supervisor, human resources personnel, or PCIT.
- Use of personal devices including computers, network devices, or any other personal equipment to make a direct network connection (wired or wireless) to Plumas County information systems within Plumas County facilities is prohibited.
- Personal devices such as mobile phones and tablets may be used to access Plumas County technology such as email, calendar, and unified communications and for purposes of multi-factor authentication. Personal devices may be denied access if insecure configurations are detected (e.g., a jailbroken phone, or a phone that does not use a password/PIN). Plumas County reserves the right to require personal mobile devices or mobile apps to be managed by a mobile device or mobile app management solution to protect Plumas County's technology and data.
- Use of information systems to solicit for commercial ventures, religious or political causes, or for personal gain unrelated to the processes of working for or on behalf of Plumas County is prohibited unless explicitly allowed by Plumas County policy or federal, state, or local law.
- Plumas County's assets must never be left unattended in an unsecured location (e.g., at the airport, or in a coffee shop). A secured location can be a locked vehicle (out of sight if possible), your home (secured from the use by family members and guests), or within designated areas in Plumas County facilities such as an assigned cubicle or equipment storage location. Please review Plumas County's Emergency Telecommuting Policy for further information regarding secured location requirements when telecommuting.
- When working remotely or in a Plumas County facility, workforce members must lock or log out of Plumas County technology assets like laptops when not in use to prevent an unauthorized individual from obtaining data or information. When working with regulated data, workforce members must take additional precautions (e.g., positioning the equipment so the screen cannot easily be viewed or using a screen protector) to prevent others from being able to view the information on the screen while in use. When regulated data is being communicated through phone calls or spoken aloud, workforce members must take precautions (e.g., closing a door, asking people to step out for a few moments, using a headphone, speaking softly, or finding an alternative way to communicate the information) to prevent access by unauthorized parties.
- Lost or stolen Plumas County technology assets must be reported immediately by opening a ticket with the helpdesk. Your department or agency may have additional procedures for lost or stolen assets. Please speak with your supervisor to determine what these additional procedures may be.
- Upon termination of any Plumas County workforce member, including a third party or contractor, all Plumas County technology assets must be returned to Plumas County.
- Hardware and software must be procured per Plumas County procurement policies, in compliance with PCIT policies and standards, and properly licensed and registered in the name of Plumas County.

- The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Plumas County.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Plumas County or the end-user does not have an active license are strictly prohibited.
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted before the export of any material that is in question.
- Introduction of malicious programs into the network or server environments (e.g., viruses, worms, Trojan horses, rootkits, etc.).
- **Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.**
- Using a Plumas County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction or Plumas County’s Harassment, Discrimination, Retaliation Policy.
- Making fraudulent offers of products, items, or services originating from any Plumas County account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Plumas County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Plumas County or connected via Plumas County's network.

Personal Use

Plumas County technology assets are purposed for conducting the business of Plumas County. Occasional personal use of technology equipment issued to workforce members is permitted (e.g., phones and/or unified communication systems, workstations and peripherals like keyboards, monitors, mice, printers, copiers, and fax machines) if the use:

- Does not introduce additional financial costs to Plumas County;
- Does not interfere with your assigned job duties;
- Does not preempt or interfere with Plumas County service delivery; and,
- Does not otherwise violate Plumas County, departmental, or agency policies.

Information created, processed, sent, received, or stored during personal use of Plumas County technology assets will not be handled differently by Plumas County. Use of the Internet/Intranet via the County's system must withstand public scrutiny. Such information may be subject to Plumas County policies, and federal, state, and local laws including Chapter 3.5 of Title 1, Division 7 of the California Government Code (Public Records Act). A public record is any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. Cal. Gov't Code § 6252. The CPRA applies to information processed, sent, and stored on the Internet/Intranet. Additionally, records of Internet/Intranet use may be requested during litigation discovery. No use of licensed or copyrighted material should be made without permission from the holder of the license.

Personal files should not be permanently stored on Plumas County technology assets. **Plumas County is not responsible for backing up or recovering personal data.**

Acceptable Use of the Internet/Intranet

The Internet/Intranet has become an increasingly important source of information for County employees. Many County employees, and occasionally others such as contractors and volunteers, are provided access to the Internet/Intranet to assist in the performance of their work for the County. However, the diversity of information available on the Internet brings with it the potential for abuse.

You are representing Plumas County when using Plumas County's technology to access the internet, and some types of activities on the internet can pose a security risk to Plumas County's technology assets. You are responsible for ensuring that your use of the internet is appropriate, ethical, lawful, and within the scope of your employment at Plumas County.

Plumas County reserves the right to block access to internet websites and addresses, including malicious internet websites or internet addresses unrelated to Plumas County's business. Blocked websites may include possibly malicious or hacked websites, websites that contain inappropriate or offensive content, or websites provided from geographic locations known to be hostile to the United States. These websites could lead to the disclosure of non-public information. You may submit a ticket to the helpdesk to unblock websites for legitimate business usage.

Plumas County may restrict internet use to reserve bandwidth and resources for critical Plumas County services during an emergency or severe internet service impact regardless of the legitimacy of the content. Plumas County may monitor and log the use of the internet by technology assets connected to Plumas County-operated networks to comply with various laws, legal proceedings, or internal policy, to troubleshoot and support technology, or to monitor and investigate the unauthorized activity. This includes, but is not limited to:

- Use of monitoring tools installed locally on a workstation;

- Analysis of various logs generated by the user or system activity (such as proxy servers, network devices, authentication and directory servers, intrusion prevention/detection devices, firewalls, web/file servers, and other systems as necessary); and,
- Traffic analysis on inbound or outbound network traffic, including the interception, decryption, and inspection of encrypted traffic.
- Use of the Internet/Intranet is restricted to official County business purposes only defined as "Assignments given by supervisors and/or department heads requiring the use of the internet/intranet."

Passwords should NOT be shared with anyone and account sharing is prohibited.

Access to the Internet/Intranet is provided as a business tool, however, its reasonable, incidental use for personal purposes is acceptable, so long as such use does not interfere with the performance of work duties or the operation of County information systems.

No employee, however, may use the Internet/Intranet for inappropriate purposes, such as but not limited to the following:

- Personal profit, including commercial solicitation or conducting or pursuing their business interests or those of another organization.
- Unlawful or illegal activities, including the downloading of licensed material without authorization, or downloading copyrighted material from the Internet/Intranet without the publisher's permission.
- To access, create, transmit, print, download, or solicit material that is or may be construed to be harassing or demeaning toward any individual or group for any reason, including based on race, color, sex, age, creed, disability, marital status, national origin, religion, pregnancy, gender, gender identity or expression, genetic information, sexual orientation, veteran or military status, use of a service animal, or any other status protected by federal, state and local law.
- To access, create, transmit, print, download or solicit sexually-oriented messages or images.
- The knowing propagation or downloading of viruses or other contaminants.

Access to Usage Records

Employees should have no expectation of privacy in their usage of the Internet/Intranet. An audit authority designated by a department head may monitor the usage of the Internet/Intranet by department employees, including reviewing a list of sites accessed by an employee within the department; an audit and examination of usage by an agency or department head shall be performed by a person designated by the County Administrator. For this purpose, records of access to sites, materials, and services on the Internet/Intranet may be recorded and retained for a time set by the County. The County or Department Head may restrict access to certain sites that it deems are not necessary for business purposes.

This policy does not supplant the legal protections available to shield confidential, internal County communications from third-party requests, such as information exempt from disclosure under the CPRA, shielded by attorney-client privilege, or subject to a state law mandating confidentiality for the specific subject matter.

Do not use your Plumas County email address as the account information for any personal accounts used to access internet services, websites, and social media (e.g., LinkedIn). You must use separate credentials and your personal email address for those activities. You may use your Plumas County email address as a username when creating an account related to your employment responsibilities at Plumas County.

Acceptable Use of Electronic Messages

Malicious individuals often use email when trying to acquire Plumas County customer data, non-public information, and data, or to compromise Plumas County's technology assets. You are required to use Plumas County messaging applications (e.g., email, instant message, text messaging, etc.) in the following professional manner:

- Not all workforce members are authorized to access the same data. Accounts are issued solely for the use of the individual to whom the account has been assigned. Sharing individual account information may lead to unintentional disclosure of data and is prohibited.
- Shared mailboxes where an authorized workgroup can monitor emails sent to and from the shared mailbox are allowed. A shared mailbox is a type of user mailbox that doesn't have its username and password. As a result, users can't log into them directly. To access a shared mailbox, users must first be granted "Send As" or "Full Access" permissions to the mailbox. Once that's done, users sign in to their mailboxes and then access the shared mailbox by adding it to their Outlook profile.
- Administrative delegation of access to an individual email account is acceptable (e.g., an executive or administrative assistant, or a peer), if this is accomplished through the email system's delegation functionality and not by sharing credentials.

If you have doubts or serious concerns about the origin or authenticity of an electronic message, or if you receive a highly abnormal or suspicious message, you should report the message by submitting a ticket to the helpdesk. Your department or agency may have additional reporting requirements so check with your supervisor.

Use caution when opening emails and attachments, particularly those received from an external sender.

- Don't open any attached files or click on hyperlinks to download files containing macros, scripts, or executables from an unknown or suspicious source.
- Malicious messages often appear to come from a valid source and could attempt to make you disclose personal or sensitive information. Use caution when opening attached files or clicking on hyperlinks, or when unusual requests or information is included in the email even if from a familiar sender.
- Training will be provided on detecting malicious emails to all Plumas County workforce members. Additional training may be required if there is repeated susceptibility to malicious emails by individuals.
- Do not forward Plumas County email containing confidential, sensitive, or regulated data to personal email accounts.
- Automatic forwarding of email through the use of rules to any external domain (non-countyofplumas.com or other Plumas County-owned and operated domains) requires approval by PCIT and can be requested by opening a ticket with the helpdesk.
- Do not send fictitious or forged messages that could be mistaken for official Plumas County statements, marketing, or materials.
- Do not send junk mail or chain letters.
- Do not use profanity, inappropriate language, pornography or sexually explicit material, slanderous, discriminatory language, harassment, or misleading content.
- Do not use Plumas County messaging applications to send unprofessional, threatening, libelous, or derogatory messages.

Acceptable Use of Voice Communications Systems

Plumas County's phone and communication systems are provided to facilitate business activities. Similar to internet browsing and other computing activities, phone call information and metadata (e.g. Caller ID, Date and Time of Call, Call Duration) may be monitored and logged.

- If the call will be recorded, you must notify all call participants that the call will be monitored or recorded, including the purpose of recording at the outset of the recording and include the notification in the recording. This does not apply to lawful monitoring or recording that does not require consent per federal, state, or local law (e.g., Cal Penal Code Section 633). Voicemail or other automated telephony system recordings comply with this section if the recorded greeting indicates that the caller has reached a voicemail system or is about to be recorded.
- Call recordings containing sensitive or regulated data presents serious security and compliance risk and should be avoided. Departments or agencies that will purposefully and continuously record sensitive or regulated data such as payment card data or protected health information must notify PCIT unless explicitly authorized in federal, state, or local law (e.g., calls to 911).

Acceptable Use of Wireless Networks

Not all wireless networks are configured with strong security protections. In addition, unauthorized and malicious wireless devices may pose a risk to Plumas County technology assets. While performing your role at Plumas County:

- Direct connections (i.e., directly connected to internal wireless access points or physical network infrastructures like a data jack in a wall plate or a network switch port) to Plumas County's protected internal private wired and wireless network are provided only to Plumas County workforce members using Plumas County-owned and operated technology assets. Third parties, vendors, contractors, and other non-Plumas County personnel access to Plumas County's protected internal private wireless or wired network is prohibited without prior approval by PCIT who may employ security measures to prevent unauthorized network connectivity. If an exception is required for a legitimate business need please open a ticket with the helpdesk.
- Third-party internet access (such as access provided at airports, hotels, and coffee shops) carries potential security risks to Plumas County technology assets. Special care should be taken to ensure you are connecting to the correct network and not bypassing any security alerts and warnings.
- Plumas County's wireless network infrastructure may only be altered and managed by authorized PCIT personnel.
- You must not install, connect, or modify any wireless infrastructure such as Wireless Access Point (WAPs) to Plumas County's network without explicit written authorization from the PCIT.

Acceptable Use While Utilizing Remote Access Technology

Remote access to Plumas County's applications is available for workforce members to work outside of the office or for telecommuting. While using remote access:

- Ensure you do not type any remote access passwords while someone is watching.
- Only store passwords in a password manager or browser configuration approved by PCIT.
- Do not leave technology assets unattended and remotely logged on to Plumas County's network. When not in use, store your equipment and media used to remotely access Plumas County systems in a secured location.
- **Do not share passwords, smart cards, tokens, keys, fobs, or any other access or authentication devices with any other person.**
- Vendors must be limited to the minimum amount of privilege and access required to perform the necessary duties while using remote access methods approved by PCIT.
- Remote support sessions must first be authorized by PCIT support personnel before the session is established and terminated as soon as the vendor has finished their work.
- No vendor may be given remote access that is not strictly controlled and monitored.

- Vendors shall not be given permanent remote access to Plumas County's network unless that access is strictly limited to the systems supported by the vendor and controls are in place to monitor their activities to ensure they are not able to gain additional access to other Plumas County technology assets from the systems they can remotely access.

Remote access to technology assets that contain sensitive or regulated data requires multi-factor authentication and the use of a secure connection between the host and the remote device.

- You must not use remote access products like TeamViewer, GoToMyPC, or similar products unless approved by PCIT.
- Do not use unsecured public or private wireless networks. Do not bypass warnings that indicate the wireless network is not secure.

Acceptable Use of Social Media

Employees of Plumas County may be able to access social media services and social networking websites at work, either through company IT systems or via their equipment for work purposes.

This social media policy describes the rules governing the use of social media at Plumas County and describes how employees conduct themselves when using Plumas County/Plumas County Department social media accounts. It also explains the rules about using personal social media accounts at work and describes what staff may say about the County/Department on their personal accounts.

Social media sites and services include (but are not limited to):

- Popular social networks like **Twitter** and **Facebook**
- Online review websites like **Reevoo** and **Trustpilot**
- Sharing and discussion sites like **Reddit**
- Photographic social networks like **Instagram**
- Question and answer social networks like **Quora** and **Yahoo Answers**
- Professional social networks like **LinkedIn**

Why this policy exists

Social media can bring significant benefits to Plumas County/Plumas County Departments and the community, particularly for building relationships with residents who may seek services or benefit from programs.

However, employees who use social media within the County/Department must do so in a way that aligns with the Plumas County/Plumas County Department's mission and values.

An inappropriate status update can generate complaints, alienate residents, or damage Plumas County and/or Plumas County Department's reputation. There are also security, privacy, and data protection issues to consider.

This policy explains how employees can use social media safely and effectively.

Responsibilities

Everyone who operates a Plumas County/Plumas County Department social media account or who uses his/her personal social media accounts at work has responsibility for implementing this policy. Some staff within each County Department may have key responsibilities in managing social media. Each County

Department is in charge of managing its own social media pages but **must notify I.T. so that the social media account can be added to ArchiveSocial, our public record request archive.**

General Social Media Guidelines

- **The power of social media**
  Plumas County recognizes that social media offers a platform for the County and County Departments to conduct outreach; stay connected with clients and the community, and build its reputation online. Plumas County also believes its employees should be involved in relevant conversations on social networks. Social media is an excellent way for employees to make useful connections; share well-researched information and shape discussions.
- **Basic guidelines**
  Regardless of which social networks employees are using, or whether they are using the agency or personal accounts on company time, following these simple rules helps avoid the most common pitfalls:
  - **Know the social network.** Employees should spend time becoming familiar with the social network before contributing. It is important to read any FAQs and understand what is and is not acceptable on a network before posting messages or updates.
  - **If unsure, do not post it.** Staff should err on the side of caution when posting to social networks. If an employee feels an update or message might cause complaints or offense - or be otherwise unsuitable - they should not post it. Staff members can always consult their supervisor or Department Head for advice.
  - **Be thoughtful and polite.** Many social media users have gotten into trouble simply by failing to observe basic good manners online. Employees should adopt the same level of courtesy used when communicating via email.
  - **Look out for security threats.** Employees should be on guard for social engineering and phishing attempts. Social networks are also used to distribute spam and malware. (Further details below.)
  - **Keep personal use to break time.** Plumas County believes that having employees who are active on social media can be valuable both to those employees and to the County or County Departments. Personal use should only happen during break time.
  - **Keep work and personal accounts separate.** It can be tricky when you know clients through work and outside of work. Keep accounts separate by using County/County Department accounts for work-related posts, and personal accounts for personal posts.
  - **Do not make promises without checking.** Some social networks are very public, so employees should not make any commitments or promises on behalf of the Plumas County Department without checking that the County/Department can deliver on the promises. Direct any inquiries to the Department Head.
  - **Handle complex queries via other channels.** Social networks are not a good place to resolve complicated inquiries and client issues. Once a client has made contact, employees should handle further communications via the most appropriate channel - usually email, telephone, or private message.
  - **Do not escalate things.** It is easy to post a quick response to a contentious status update and then regret it. Employees should always take the time to think before responding and hold back if they are in any doubt at all.

Use of Department/County Social Media Accounts

This part of the social media policy covers all use of social media accounts owned and run by Plumas County/Plumas County Departments.

- **Authorized Users**

- Only people who have been authorized to use Plumas County/Plumas County Department social networking accounts may do so.
- Authorization is provided by the Department Head. It is granted when social media-related tasks form a core part of an employee's job.
- Allowing only designated people to use the accounts ensures the County/Department’s social media presence is consistent and cohesive.

- **Creating Social Media Accounts**
  - New social media accounts in a Plumas County/Plumas County Department’s name must not be created unless approved by the Department Head.
  - If there is a case to be made for opening a new account, employees should raise this with their Department Head.

Purpose of Social Media Accounts

Plumas County/Plumas County Department’s social media accounts may be used for many different purposes.

Employees should only post updates, messages, or otherwise, use these accounts when that use is clearly in line with the County/Department’s overall mission and objectives. For instance, employees may use company social media accounts to:

- Respond to community inquiries and requests for help, articles, and other content created by County Departments or other vetted sources, share insightful, well-researched articles, videos, media, and other content relevant to the County Department, but created by others, and provide fans or followers with an insight into what goes on at Plumas County/Plumas County Departments. Social media is a powerful tool that changes quickly. Employees are encouraged to think of new ways to use it and to put those ideas to the Department Head.

Inappropriate Content and Uses

Plumas County/Plumas County Department social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the Department into disrepute. Inappropriate content includes pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling, and illegal drugs.

Employees must not share personal grievances with co-workers on the Plumas County, Plumas County Department, or personal social media pages.

When sharing an interesting article or piece of content, employees should always review the content thoroughly, verify the source as reputable, and should not post a link based solely on a headline.

Personal Social Media Rules

Acceptable use:

- Use of social media accounts for non-work purposes is restricted to non-work times, such as breaks and during lunch.
- Talking about the County/Department:
  - Employees must clarify that their social media account does not represent Plumas County/Plumas County Department's views or opinions.
  - Staff may wish to include a disclaimer in their social media profiles: 'the views expressed are my own and do not reflect the views of my employer.

Copyright

Plumas County/Plumas County Departments must respect and operate within copyright laws. Users may not use social media to:

- Publish or share any copyrighted software, media, or materials owned by third parties, unless permitted by that third party.
- Share links to illegal copies of music, films, games, or other software.
- *If staff wish to share content published on another website, they are free to do so if that website has obvious sharing buttons or functions on it.

Security and Data Protection

Employees should be aware of the security and data protection issues that can arise from using social networks.

- **Maintain confidentiality**
- **Users must not:**
    - Share or link to any content or information that could be considered confidential.
    - Share or link to any content or information owned by another company, agency, department, or person that could be considered confidential.
- **Protect social accounts:**
    - Company social media accounts should be protected by strong passwords that are changed regularly and shared only with authorized users.
    - Staff must not use a new piece of software, app, or service with any of the Plumas County/Plumas County Department social media accounts without receiving approval from the Department Head.
- **Avoid social scams:**
    - Staff should watch for phishing attempts, where scammers may attempt to use deception to obtain information relating to either the company or its customers.
    - Employees should never reveal sensitive details through social media channels. Customer identities must always be verified in the usual way before any account information is shared or discussed.
    - Employees should avoid clicking links in posts, updates, and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague-sounding direct messages.
    - Do not seek to influence a politician or public official on an issue through social media campaigns.

Electronic Signature Use

The Countywide eSignature Policy shall be used by Plumas County Agencies and Departments to increase productivity and ensure convenient, timely, and appropriate access to County information by using electronic signature technology to collect and preserve signatures on documents quickly, securely, and efficiently.

This Policy establishes when electronic signature technology may replace a hand-written signature, to encourage the use of paperless, electronic documents whenever appropriate and allowed by law. This Policy applies to all signatures used in processing various County documents and assumes the County signer has been given the authority to sign as determined by Agency/Department business process and the County Purchasing Policy.

While the use of electronic signatures is suggested and encouraged, this Policy does not require any Agency/Department to use electronic signatures, nor can the County mandate that any third party signs a document using an electronic signature.

Background/Discussion

Electronic Signature is the broad umbrella category under which all electronic signatures fall.

The legality and use of Electronic Signatures are governed by federal and state law. (See 15 U.S.C. §§ 7001, et seq. [U.S. Federal Electronic Signatures in Global and National Commerce Act]; California Government Code §16.5; California Civil Code §§ 1633.1, et seq.)

Intended Goals for eSignature

- **Security and Legal Compliance:** The use of e-forms and e-signature provides a secure method of signing and transferring documents electronically. A document cannot be altered after the signer has completed the e-signature. Additionally, a history of any changes made to the document before the signature is kept with the document and cannot be changed or deleted. When electronic signatures are used, hash values are attached to the document to verify the authenticity of a document during any transfer for added security.
- **Integration into business processes:** The eSignature process may fit into pre-existing business practices, provide automated processes, retrieve documents, use standard Application Program Interfaces (API), generate reminders and expiration settings, and allow multiple people to view a document and track its progress.
- **Simplified workflow**: E-signatures eliminate resource-intensive processes that require agencies, the public, and staff to manually sign documents. Features of the e-signature process include automation of simple forms, the ability to track and review changes, varying the recipient roles, tag signatures, etc.
- **Cost benefits:** There is a potential cost saving from not having to print, file, scan, and store paper copies. The County will save also on certified mail, postage, printing, ink, envelopes, and paper.

Policy

This Policy applies to documents requiring a signature of any person where the signature is intended to show authorship, approval, authorization, or certification, as allowed by law. It is the policy of the County to encourage the use of electronic signatures in all internal and external activities, documents, and transactions where it is operationally feasible to do so, where existing technology permits, and where it is otherwise appropriate based on the Department's preferences. In such situations, affixing an electronic signature to the document in a manner consistent with this Policy shall satisfy the County’s requirements for signing a document. As used in this Policy, the term "signature" includes using initials on a document instead of a signature.

Implementation Procedures

E-signatures may be implemented using various methodologies depending on the associated risks that may include fraud, non-repudiation, and financial loss. The quality and security of the e-signature method should be commensurate with the risk and any requirements to assure the authenticity of the signer.

Agency/Department Discretion

Each Department has the discretion to decide whether to permit the use of electronic signatures. Departments should work with County Counsel to determine where applicable laws permit an electronic signature to be used. In addition, each Agency/Department that opts to use electronic signatures must adopt/amend their business practices to support the requirements of this Policy.

Requirements of eSignature

The use of electronic signatures is permitted and shall have the same force and effect as the use of a "wet" or manual signature if all the following criteria are met:

- The electronic signature is unique to the person using it.
- The electronic signature is capable of verification.
- The electronic signature is under the sole control of the person using it.
- Email notifications requesting electronic signatures must not be forwarded.
- These requirements prohibit the use of proxy signatures.
- The electronic signature is linked to the data in such a manner that if the data is changed after the electronic signature is affixed, the electronic signature is invalidated.

Document Type Examples	Is Use of an Electronic Signature Acceptable?	Notes
Memos, Forms, Board Letters, and Other Correspondence	Yes	Electronic Signature is recommended.
Contracts, excluding contracts of $10,000 or more	Yes	Electronic Signature is recommended.
Certificates, Permits	Yes, if allowed by law	Departments should work with County Counsel to determine where applicable laws permit an electronic signature to be used.
Documents Requiring Notarization	No	
Document Requiring the Board Chair's Signature	No	

Common Types of Documents

This Policy is intended to broadly permit the use of electronic signatures. Examples of common types of documents are listed in the table above, with notes on each type of document. Agencies/Departments should work with County Counsel to determine where applicable laws permit an electronic signature to be used.

Documents Involving Other Parties

In the case of contracts or transactions which must be signed by outside parties, each party to the agreement must agree in advance to the use of an electronic signature. No party to a contract or other document may be forced to accept an electronic signature; they must be permitted to decide either way. Such consent may be withdrawn by the other party at any time such that future documents must be signed in hardcopy format.

When a document is electronically signed by all parties, the County will provide a copy of the electronically signed document to the other parties in an electronic format that is capable of being retained and printed by the other parties.

Setup & Use

To set up employees authorized to send out documents for eSignature, Agency/Department Security Administrators should contact PCIT.

Storage and Archiving of Electronically Signed Documents

If a document exists only electronically, steps should be taken by each Agency/Department to ensure that a fixed version of the final document is stored in some manner. It is up to the Department to decide how to store these final electronic documents so long as it does so in a manner consistent with any applicable County document retention policies and any applicable laws.

eSignature Solution Providers

The Plumas County Information Technology Department will be responsible to determine acceptable technologies and eSignature providers consistent with current state legal requirements and industry best practices to ensure the security and integrity of the data and the signature.

Conclusion

The use of e-Signature is intended to make Plumas County business practices more efficient. The process eliminates the need to print, file, and store paper copies of documents that can now be authenticated digitally and stored electronically.

Multi-Factor Authentication Policy

The purpose of a Multi-Factor Authentication (MFA) Policy is to enable a means of strong authentication for those users with access to sensitive information and information systems resources or have a privileged level of system support access while ensuring ease of use and adoption for the user(s). The adoption of a Multi-Factor Authentication (MFA) Policy will reduce the likelihood of unauthorized access, provide demonstrated compliance to federal and industry mandates, as well as enable the solicitation, assessment, and selection of MFA solutions that will implement the requirements of this policy. The purpose of this policy is to define requirements for accessing County of Plumas computer systems, including, but not limited to Microsoft 365 email services, and Virtual Private Networks (VPNs) containing sensitive data from both on and off-campus. The standards outlined in this policy are intended to minimize potential security risks which may result from unauthorized use of the County of Plumas computing resources.

The goals of this policy are as follows:

- 1. Protect the identities of the County of Plumas systems from compromise.
- 2. Protect the security, confidentiality, and integrity of computing network accounts.
- 3. Protect system administration accounts from misuse.

The goal of multi-factor authentication is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a computing device, network, or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

User requirements

- Register a device that can receive push notifications or codes via the FREE Microsoft Authenticator Mobile app.
- When users attempt to log into a County of Plumas system protected by multi-factor authentication, the system will “challenge” the user by requesting a second factor of authentication. This second factor could be an acknowledgment of a push notification, a code, or a physical token. This second factor will be provided through the secure method(s) the user selected during registration.
- It is the user’s responsibility to promptly report compromised credentials to Plumas County Information Technology (PCIT).

Registration

Users will use the multi-factor authentication self-enrollment process to register their authentication device(s) and install the FREE Microsoft Authenticator Mobile app. More information is available in the process guide https://plumascounty.us/DocumentCenter/View/41389/MFA-Instructions.

Devices

The preferred method for delivering access codes and/or push notifications is via the Microsoft Authenticator mobile app, which can be installed on any supported smartphone or tablet. The Microsoft Authenticator app is the preferred and recommended solution for County of Plumas users. Users are encouraged to use personally owned smartphones or tablets for the Microsoft Authenticator mobile app. The use of jailbroken/rooted devices is prohibited.

Receiving Microsoft multi-factor authentication codes via SMS is an option for users who cannot access a smartphone or tablet but do own a mobile device capable of receiving SMS messages, but users are encouraged to use the Microsoft Authenticator mobile app if possible.

Microsoft Authenticator may, at its discretion, drop app support for older versions of mobile operating systems. Microsoft maintains the full list of supported devices.

Lost or Stolen Devices

If a user's registered device is lost or stolen, or the user has reason to suspect their Plumas County Online ID credentials have been compromised, the user must contact PCIT IMMEDIATELY.

Off-Hours and Emergency Access to Protected Data

PCIT shall maintain internal procedures for processing emergency access requests if issues arise with the multi-factor authentication process. Users should contact PCIT for access.

Exclusions for Special Circumstances:

There may be situations in which an employee of the County of Plumas has a legitimate need to utilize Plumas County technology resources outside the scope of this policy. The IT Department Head may approve, in advance, exception requests based on balancing the benefit versus the risk to the County. Exception requests must be made through the FreshService ticketing system. Policy exception requests shall be made to the IT Department Head and include a brief description of the system and/or type of data access requested. Please be certain to indicate if the user handles Personally Identifiable Information (PII) or other confidential information, such as electronic protected Health Information (ePHI), financial data, credit card payments, Social Security numbers, or works with children.

Due to the evolving nature of technology, cyber threats, and the changing roles of users at the County of Plumas, all exemptions will be reviewed periodically and at the discretion of the IT Department Head in collaboration with IT staff. This review will verify that the need stated in the request is still valid and/or that the user still requires the approved multi-factor exempted access.

Consequences:

Failure to register a device will result in an inability to use multi-factor authentication. If multi-factor authentication is required for a system, the user will not be allowed to authenticate and use the system.

Users may not attempt to circumvent login procedures, including Microsoft multi-factor authentication, on any computer system or otherwise attempt to gain unauthorized access. Attempts to circumvent login procedures may subject the user to disciplinary action including, but not limited to, suspension of the user's access to the electronic information resources. Financial losses incurred due to the use of Microsoft multi-factor circumvention techniques are the responsibility of the user, and the County may seek financial restitution from users who violate this policy.

VI. No Expectation of Privacy

Plumas County must monitor all systems and users of technology assets to maintain a secure environment and meet compliance requirements. You should not expect privacy or confidentiality while using Plumas County technology assets, including internet access and emails. Usage may be monitored for policy, security, or network management reasons and is subject to inspection at any time. Inspection and monitoring of Plumas County technology assets by management does not require the consent of individual workforce members.

All electronic messages or data created, stored, transmitted, or received over Plumas County systems or through Plumas County internet connections are subject to inspection or monitoring. Plumas County reserves the right to store and/or access the contents of any messages or data sent over its networks and use that information to enforce its policies or comply with federal, state, or local law. If the content violates regulations or laws, Plumas County reserves the right to submit the information to law enforcement for potential prosecution.

VII. Reporting Known or Suspected Vulnerabilities or Security Incidents

You must report known or suspected security weaknesses, instances of inappropriate access, and suspicious activities to PCIT by opening a ticket with the helpdesk. Your department or agency may also have reporting requirements so please check with your supervisor.

You will be responsible for the confidentiality, integrity, and availability of your files. If concerning circumstances occur with your files such as inappropriate access, loss of the files, or changes are made to files without your consent please speak with your supervisor and report this issue by opening a ticket with the helpdesk.

You must report suspicious activities happening to or on your workstation such as someone remote controlling the workstation without your consent or new and unfamiliar software performing unusual activities by opening a ticket with the helpdesk.

VIII.Maintenance

This policy will be maintained by PCIT. This includes, but may not be limited to:

- Interpretation of this policy
- Ensuring this policy content is kept current
- Recommending updates to this policy and related resources
- Developing an escalation and mitigation process if a Department is not in compliance
- Assisting Organizations to understand how to comply with this policy
- Monitoring annual compliance by Departments

IX. Consequences for Noncompliance

Violations of this policy may be grounds for disciplinary action, up to and including termination and enforcement action which may include civil or criminal charges. Any improper technology asset usage will not be disclosed by the County to others except to the extent necessary to consider and implement discipline, for other employment-related purposes, or to respond to litigation requests. Potential criminal conduct which is revealed by improper technology asset usage will be referred to the appropriate law enforcement authorities.

X. Acceptable Use Policy and Standards Glossary

Acceptable Use: A term referring to the usage of Institutional Information and IT Resources that complies with Plumas County's security, privacy, and ethics policies.

Archive: Data that has been removed from the storage system to another (off-line) location for historical purposes, available for reference or recovery on an as-needed basis. The archive medium may be different from that of the previously stored data, may be in a different physical location, and may, depending on the media and software used, be usable only after it has been run through a "restore" process.

Authentication: The process by which you prove your identity to another party. "Authentication is the act of confirming the identity of an individual by verification of the digital credentials presented by the individual when accessing a resource. An *authentication credential* may be:

something the individual knows, such as a password, passphrase, or other secret information

something the individual has, such as a smart card with a public-key certificate

something that is biologically part of the individual, such as a fingerprint or a retina

Breach (Breach of Security): Any confirmed disclosure or unauthorized acquisition of County Information that compromises the security, confidentiality, or integrity of County Information maintained by Plumas County. Good faith acquisition of personal information by a County employee or agent for County purposes does not constitute a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Backup: A copy of data as it existed at a specific point in time. The backup is held on physically different media (but may be of the same type) as the active data set. Backup data may depend on the medium and backup software used, and be usable only after it has been run through a "restore" process.

Computer Security Incident: See "Security Incident"

Device: Any electronic component, such as a computer, printer, router, switch, modem, PDA, etc.

Disaster recovery: Restoring a system or operational function after a service-impacting event.

Electronic Communications: Any information that is transmitted electronically. This includes, but is not limited to, email and email attachments, Google Docs, web pages, phone calls, faxes, broadcasts, electronically transmitted files, information submitted online, etc. It also applies to details about an individual's online activities, and information from transactional logs.

Electronic Protected Health Information (ePHI): protected health information (PHI) that is produced, saved, transferred or received in an electronic form. In the United States, ePHI management is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.

Email Spam Robot (spam bot): A malicious program designed to covertly send unsolicited email (spam) from computers that it infects. The spambot is remotely controlled as part of a collection, or "army," of spam engines.

Encryption: The process of converting data into a cipher or code to prevent unauthorized access. The technique obfuscates data in such a manner that a specific algorithm and key are required to interpret the cipher.

Essential Resource: A resource is designated as Essential by Plumas County if its failure to function correctly and on schedule could result in

A major failure by a Campus to perform mission-critical functions

A significant loss of funds or information

A significant liability or other legal exposure to a Campus.

A system required for the operation of a major function is an essential system.

File recovery: Restoring individual files or records from original, archive, or backup media.

FTP: “File Transfer Protocol.” A non-secure method of transferring files between computers on a network. The currently preferred alternative is SFTP.

HIPAA: Federal Health Insurance Portability and Accountability Act. HIPAA Privacy and Security Laws mandate protection and safeguards for access, use, and disclosure of protected health information and/or ePHI with sanctions for violations.

HIPAA Data: See Electronic Protected Health Information (ePHI)

HTTP: “Hypertext Transfer Protocol.” The communication protocol (language) enables web browsing.

HTTPS: “Secure Hypertext Transfer Protocol.” An acronym used to indicate a secure, encrypted HTTP connection.

IMAP: “Internet Message Access Protocol.” A mail protocol that provides access to email and management of email messages on a remote server.

IMAPS: Secure, encrypted IMAP.

Information Security Event: An identified occurrence in a system, service, or network state indicating a possible breach of information security policy, a failure of controls, or a previously unknown situation that may be relevant to security.

Infected Computer: A computer containing any type of malicious software.

Information Security Incident Response Plan: An Information Security Incident Response Plan is a written document detailing the steps required to address and manage an Incident or cyber-attack. A response plan is one part of a Security Program.

Information Security Incident Response Program: The full, comprehensive effort to identify, prevent, prepare for, respond and recover from Incidents or cyber attacks

Integrity: The consistency, accuracy, and trustworthiness of data over its entire lifecycle. Integrity is one of the 3 elements of the "CIA Triad" security model (Confidentiality, Integrity, and Availability).

IT Resource: A term that broadly describes IT infrastructure, software, and/or hardware with computing and networking capability. These include, but are not limited to, personal and mobile computing systems and devices, mobile phones, printers, network devices, industrial control systems (SCADA, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic and physical media, biometric and access tokens, and other devices that connect to any County network.

Malicious Software, or "malware": A generic term for software that performs unauthorized activities on a computer, causes damage, or allows unauthorized access to be gained. Examples of malicious software include viruses, spyware, and email spam robots.

Multi-Factor Authentication (MFA) is a method of computer access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something the user knows), possession (something the user has), and inherence (something the user is).

Network Service: A resource running on a device that can be shared by other computers. Examples include web servers, mail servers, file sharing, remote connectivity capability, and servers.

Password: A string of characters (letters, numbers, and/or symbols) used to authenticate an identity, verify access authorization, or derive cryptographic keys. Generally composed of not more than 8-16 characters.

Privileged Access: Privileged access is any access to systems, applications, databases, etc. that enables a user to carry out system administration functions, or that provides broad access to personal or County data (beyond just the user's data).

Privileged User/Accounts is a User/Account that by function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and Network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

Procedure: A collection of steps or processes that describe how the requirements of a specific job task, policy, or standard are met.

Public Information: Public information is any information relating to the conduct of the public's business. In the case of personal information, the term relates to information that has been determined not to constitute an unwarranted invasion of privacy if publicly disclosed.

Risk Assessment: A process to identify, rate, and prioritize risk, as well as to document risk tolerance.

Security Incident: A compromise of the confidentiality, integrity, or availability of Institutional Information in material or reportable way. A single event or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations or threatening information security.

Sensitive Data: Sensitive data is an informal term used to describe information with some level of sensitivity.

Session Timeout: A process that automatically prevents user access to a system or application after a period of inactivity. The purpose of timeouts is to lock out unauthorized users when a system is unattended or when someone forgets to log out of an application.

SFTP: “Secure File Transfer Protocol.”

A program that is similar to FTP and uses SSH to transfer files. Unlike FTP, SFTP encrypts both the session and the password so nothing is sent in clear text form. This prevents an eavesdropper from capturing or stealing passwords or data as they travel over the network.

A secure, encrypted method of transferring files between computers on a network.

SMTP: “Simple Mail Transfer Protocol.” The *de facto* standard for email transmissions across the Internet. SMTP is a text-based protocol, where one or more recipients of a message are specified and then the message text is transferred.
http://en.wikipedia.org/wiki/SMTP

SNMP: “Simple Network Management Protocol.” A protocol used by network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.
http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Spyware: Computer programs that typically track your use and report this information to a remote location. The more malicious spyware programs may capture and report keystrokes, revealing passwords and personal information. Users are often tricked into installing spyware programs without their knowledge. Spyware is sometimes referred to as adware.

Standard: Requirements that specify the set of administrative, technical, or procedural controls necessary to meet the related policy. Standards differ from the policy in that they can be more detailed and can change more rapidly in response to new technology or new or evolving threats.

System: In general, an interrelated group of electronic components, e.g. hardware and/or software, that work as a coherent entity. Concerning information security breaches, a system is any computer-readable collection of information that contains electronic data in an organized form such that information about a particular subject can be distinguished from information about other subjects.

Transactional Information: Information, including electronically gathered information, is needed either to complete or to identify an electronic communication. Examples include but are not limited to electronic mail headers, summaries, addresses, and addressees; records of telephone calls; and IP address logs. Transactional information does not include the actual contents of people's computers, files, emails, telephone conversations, etc.

Truncate: To make it shorter. This can be to reduce or eliminate the sensitivity of data, such as using the last four digits of a Social Security number instead of the entire number.

Unit: An IT, academic, research, administrative or other entity operating within Plumas County. A Unit is typically a defined organization or set of departments.

Updates: Updates “fix" an inherent flaw or security risk in an operating system (the basic program that runs a computer) or in application software. Updates are released on an as-needed basis – typically from the operating system or software vendor (such as Microsoft, Apple, or Mozilla).

User ID is a unique symbol or character string used by an information system to identify a specific user.

Virus: Computer viruses are small, self-replicating computer programs that interfere with computer operation. The effect of viruses can range from negligible to devastating, depending on what the virus program does when it runs. A virus might, for example, corrupt or delete data on a computer, spread itself to other computers, or even install a malicious program.

VPN or Virtual Private Network is a method employing encryption to provide secure access to a remote computer over the Internet.