September 20, 2016
Regular Meeting
Item #9c
Information Technology

PC & Cell Phone Policy Update

INFORMATION TECHNOLOGY STANDARDS & POLICIES

MONO COUNTY &
TOWN OF MAMMOTH LAKES, CA

PRODUCED BY
Mono County Information Technology
437 Old Mammoth Road, Suite 228
PO Box 7657
Mammoth Lakes, CA 93546

TABLE OF CONTENTS

PURPOSE OF POLICY

Mono County recognizes the value of information and the technology which we utilize in order to carry out daily business. Coupled with the laws and standards which regulate information maintained by a local agency, these policies are intended to clearly define appropriate use and indicate best practices.

The policies contained in this document are intended to be for the greater Authorized User community. In addition to this policy set, the IT Department reviews, develops, adopts, and implements a set of 'internally facing' policies that ensure overall Agency compliance with State and Federal regulations.

This manual was developed based on the unique set of operating conditions present in Mono County and the Town of Mammoth Lakes, while being aware of how other California municipalities operate. The policies are in alignment with the International Organization for Standardization ISO/IEC 27002 (Code of Practice for Information Security Management framework) and are considered to be in effect twenty-four hours a day, 365 days a year.

ROLES & RESPONSIBILITIES

Given the value and demand on the technology resource at the agencies, it is imperative that Users abide by an ethics standard that ensures that the IT department can keep systems running and ensure a safe, efficient, and effective system to work within. It is the responsibility of all County and Town personnel, elected officials, contractors, and visitors to ensure that technology is used appropriately, and that the policies, standards, and expectations expressed in this manual are followed.

Information Technology Department (IT Department)

The Information Technology Department (IT) is centralized within Mono County and the Town of Mammoth Lakes. Mono County employs a staff of IT Specialists who provide front-line support for hardware, software and technology services to Mono County, Mono County Sheriff, the Town of Mammoth Lakes, and the Mammoth Lakes Police Department (collectively referred to as "the agencies"). IT staff respond to requests for service, develop and manage various technology projects, and provide leadership, oversight, or technical direction during the implementation of new technology. IT staff also ensure the appropriate use of technology through monitoring and training, and as defined in this manual, including:

- Demonstrating best practices in technology use and information management
- Providing front line support and user training
- Making appropriate technology recommendations to the agencies and its departments
- Upholding and enforcing IT and security policies

Department Heads & Managers

Department Heads and Managers are responsible for ensuring that staff working under them understand and comply with the policies and standards set forth in this manual. This includes, but is not limited to:

- Ensuring all Users of agency technology and information are made aware of these standards and policies
- Enforcing IT and security policies by reporting any unauthorized or inappropriate use of technology and information to the IT Department
- Ensuring that their staff have the training and support necessary to perform their job
- Budgeting appropriately for the implementation and maintenance of technology within their department
- Responding to IT queries regarding the implementation of technology and information within their department

Authorized Users

Authorized Users or Users are the lifeblood of the organization and are daily users of technology and associated information. In order for the agency to be successful in business operations, it is imperative that Authorized Users (Users) be appropriately trained, qualified, and able to use technology in a manner that is compliant with the Agency standards and policies contained herein.

POLICY #1: USE OF TECHNOLOGY

This section defines the ways in which technology is used in the organizations, acceptable use, considerations, constraints and applications.

1A. Acceptable Use of Accounts, Network and Equipment

Staff are expected to exercise responsible, ethical behavior when using technology, as defined below:

1A.1: Responsibility for Accounts: Each User shall be assigned an account with a standardized login. Users are solely responsible for all usage of the assigned account. Authorized Users shall only access the computer accounts that have been authorized for use by the Agency. The unauthorized use of another User's account, or providing of false or misleading information for the purpose of obtaining access to computing, is prohibited.

1A.2: Confidentiality of Logon Credentials: Authorized Users shall not share their logon credentials with anyone. Should a User require access to a colleague's account, written authorization is required from the Department Head(s) and the CAO. Access will be granted through the sharing of said User's data by *mapping* to the User's stored information, rather than allowing for impersonation of that User.

1A.3: Data Restricted to Authorized Users: Former employees and other unauthorized users are forbidden from accessing or storing Agency data or accounts.

1A.4: Unlawful Purposes Are Prohibited: Accounts and devices are to be used for lawful purposes only. Prohibited use of Agency equipment includes but is not limited to: downloading or installing fraudulent material or software, transmitting offensive or disruptive information or material, or intentionally damaging the system. Use of the Agency network to gain unauthorized access to other areas of the network or systems to which it is connected is strictly prohibited under this policy and the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.

1A.5: Duty to Report Misuse: Any known misconduct or violation of policies shall be reported to the IT Department immediately. Authorized Users are also encouraged to report any information relating to a security concern, flaw or similar issues, upon discovery.

1B. Use of Agency Owned Devices (AOD)s, Provided Equipment, Networks, and Storage

All equipment and data provided to Authorized Users are considered Agency property and intended for business use only. Users are expected to use equipment properly and respectfully and for the purposes for which it was intended.

1B.1: Assignment of Equipment: Prior to the commencement of employment, a Department Head or Manager may request that a PC be assigned to an employee and access granted to Agency technology resources. Additionally, employees may be assigned an Agency Owned mobile device (such as a cellular or smart phone) for their regular job duties. Upon termination, all AODs must be returned to the County.

- PC acquisitions must comply with Policy 3C.
- Assignment of Agency Owned Mobile Devices is further outlined in Appendix I.

1B.2: No Expectation of Privacy: Authorized Users have *no* right of privacy when using an Agency Owned Device (AOD) or other provided technology, or while utilizing the Agency network. The IT Department monitors network traffic and devices for irregularities or illegal usage. Department Heads, managers and the IT Department (as authorized by the applicable department director) reserve the right to enter, search and monitor computer files, emails and web activity of any employee without advance notice. Data that is created, stored, or received may be accessed by IT staff at any time in order to ensure network and data integrity, monitor work flow or productivity, investigate theft or other misconduct, or inspect for unauthorized disclosure of confidential business or proprietary information or concerns of personal abuse of the system.

1B.3: Access Is for Work-related Purposes: Access to the Agencies' network, Internet connection, and storage is provided to Users for work-related purposes. Personal use of the Internet may be allowed by a Department Head . Any such use should be: (a) confined to any use that is absolutely necessary; (b) kept to a minimum and be focused; (c) to the extent practical, performed on breaks or lunch time rather than during work time.

1B.4: Access Does Not Confer Work Authorization: Access to, or use of, an AOD does not imply supervisor or Department Head approval for working outside of normal working schedule or receiving compensation for time worked.

1B.5: Use is for Job Duties: Computers, devices, and similar equipment provided to Users shall only be used for performing regular job duties. Downloading or storage of personal files on Agency PCs or storage devices is prohibited. This includes pictures, music, or other documents. Agency Owned Equipment may not be used for personal business (such as using the internet for research, printing personal documents, etc.) unless specific authorization is given by a Department Head under 1B.3.

1B.6: Do Not Remove Equipment Without Permission: Agency Owned Devices and equipment shall not be removed from the premises without prior authorization from IT. The assignment of a portable computing device (such as a laptop, tablet, or mobile device) implies such authorization.

1B.7: Mobile/Portable Devices Must Be Encrypted and Passcode Protected: An Authorized User may be provided with a mobile or portable Agency Owned Device (AOD) for certain business purposes. The device will be encrypted and a passcode required. IT will have the ability to monitor, restrict, access, and enforce use of the device. All other policies governing technology apply to Agency Owned Devices.

1B.8: Permission is Required for Software Installation: Users are prohibited from installing any software onto an Agency computer or device without gaining prior approval from the IT Department. All software installation and use must conform to licensing restrictions set forth by the vendor. Using products that are not appropriately licensed by the Agency or otherwise violate the rights of any person or organization is strictly prohibited.

1B.9: Do Not Tamper with Devices or Data: Users shall not alter or tamper with any Agency devices or data systems for any purpose. Any hardware issue or failure shall be reported to the IT Department immediately.

1B.10: Procedures in the Event of Loss or Theft of Device: If an AOD is lost or stolen, the loss or theft must be reported immediately to the IT Department so that appropriate steps may be taken.

1B.11: Follow State and Federal Laws Regarding Driving: Users must comply with all State and Federal laws governing use of mobile devices, especially those pertaining to use of mobile devices when operating vehicles or machinery.

1C. Use of Personally Owned Devices (PODs) for Agency Business

In certain circumstances it may be appropriate or necessary to utilize a Personally Owned Device (POD) for business purposes. PODs include, but are not limited to: computers, tablets, phones and other computing devices that may be connected to the Agency's network, file, or email system(s). The following rules apply:

1C.1: Devices Must Be Encrypted and Passcode Protected: Any POD that has access to an Agency mailbox mounted natively or has Agency data stored locally on the device must be password protected and encrypted. If the Authorized User accesses email through a web browser or files through a Virtual Private Network connection (VPN) and they are not stored on the device, a passcode is not required, but is recommended.

1C.2: HIPAA: Any POD used for business within a Health & Human Services Department (HIPAA covered Agency), law enforcement, or Emergency Services function, must be encrypted, must be password protected, and the User must abide by standards, laws, and regulations of HIPAA.

1C.3: Permission for Remote Access Required: Personal computers may not be plugged directly into the Agency network via Ethernet without prior authorization from the IT Department. Users may not connect PODs to the Public or Guest wireless network provided by the Agency at any time without prior consent.

1C.4: Network Use and Virus Protection: Any computer directly connecting to the Agency network must have current virus protection software on it.

1C.5: IT Support Will Be Limited: The IT Department will not provide any front-end User support for any POD unless the User is included on the Mobile Device/Cellular Stipend Program (see Appendix II) and support is needed for specific business purposes.

1C.6: Agency Not Responsible for Damage: The Agency will not repair or replace a POD if damaged while being used for Agency business. Protection of Personally Owned Devices from theft or accidental damage are the responsibility of each owner.

1C.7: Procedures in the Event of Loss or Theft of Device: If a device with Agency email or data on it is lost or stolen, the loss or theft must be reported immediately to the IT Department so that appropriate steps may be taken. The IT Department reserves the right to remotely remove the agency mailbox or wipe the device if it is directly connected to the Agency network and security has been compromised.

1C.8: Access Does Not Confer Work Authorization: Use of a POD for work purposes or Agency email access on the POD does not imply supervisor or Department Head approval for working outside of normal working schedule or receiving compensation for time worked.

1C.9: Stipends and Expectation of Access: A Department Head or Manager may determine that the use of a POD is necessary for an employee to perform their regular job duties, and authorize a stipend for that employee. In these circumstances, the Agency may expect a reasonable amount of access to the Authorized User (e.g. responding to calls or texts within the constraints of normal working schedule) or to the device (e.g. ask to have certain apps installed, use of camera, text messaging, etc. for job purposes).

- Assignment of Agency Owned Mobile Devices is further outlined in Appendix I.

1C.10: State and Federal Laws Apply: Users must comply with all State and Federal laws governing use of a Personally Owned Device, especially those pertaining to use of mobile devices when operating vehicles or machinery.

DEVICE OWNERSHIP AND MANAGEMENT MATRIX		
CATEGORY	**AGENCY OWNED DEVICES**	**PERSONALLY OWNED DEVICES**
Device Type	No Restrictions	No Restrictions
Wireless Carrier	Verizon (unless otherwise justified)	No Restrictions
Use Restrictions	Agency business only	No Restrictions
Security Requirements	Passcode & device encryption Mobile Device Management	Passcode required on device (and Encryption if Agency mailbox mounted natively or has Agency data stored locally)
IT Authority	Ability to monitor, restrict, access, and enforce. Remote wipe if device lost.	Limited Authority Remove mailbox or remote wipe if lost

Diagram 1: Differentiation between Agency Owned and Personally Owned Devices relative to management and control.

POLICY #2: SECURITY AND ACCESS

Recognizing that technology and secure information are critical for government operations, it is imperative that IT and Users collaborate to minimize vulnerability of the network, devices, and systems of confidential information.

2A. Physical Security and Protection

2A.1: Network Access and Agency Offices Must Be Secure: Access to Agency Owned or Personally Owned Devices attached to Agency network shall be restricted to Authorized Users only. Offices with such devices in them should be secured with physical locks whenever not occupied by Agency staff and monitored during normal business hours. Authorized Users may not leave mobile devices containing Agency information in locked vehicles at any time.

2A.2: Passcode Protection and Default Locking Required: Agency devices shall all be secured with a standard login method consisting of at least a username and confidential password. Devices attached to the Agency network are set to automatically lock after a specified amount of inactivity. However, Users should manually lock their device (Ctrl+Alt+Delete > Lock) whenever they step away, especially in areas to which the public may have access.

2A.3: Monitor Publicly Accessible Devices: Devices which are accessible to the public (such as kiosks, conference room computers, etc.) shall be physically secured and directly monitored by Agency staff whenever in use by the general public.

2A.4: Unauthorized Access and Use Prohibited: Authorized Users may NOT allow unauthorized users to access agency network, AOD, or agency data/information at any time.

2A.5: Security Trainings: Agency staff must attend at least one security training offered by the IT Department annually.

2B. User Accounts and Passwords

2B.1: User Accounts: The IT Department will establish a unique account for each Authorized User of the Agency's system(s). The Authorized User will create a unique password which only they know, and change it as required by IT. Passwords are required to be complex and unique and meet criteria established by the IT Department based on guidelines from the Department of Justice, HIPAA Rules & Regulations, or other compliance based policy set. For certain Users, especially those who have access to high value data or critical systems, additional security measures such as Multi-Factor Authentication may be required.

2B.2: Passwords Shall Be Kept Confidential: Users shall not distribute their passwords to anyone (including IT staff), nor provide any other User, vendor, or agency with information on accessing the Agency network. Any such requests must be referred to the IT Department. Passwords shall not be written down nor stored near workstations as they may be discovered and used to gain access to an account.

2C. Network & Data Security and Incident Reporting

2C.1: Network Access: Only devices authorized by the IT Department may be directly connected to the Agency network—this includes PODs, any device which has direct or VPN access, or otherwise provides a means for an outside party to gain access to the Agency network.

2C.2: Internet Access: In order to avoid possible virus or malware infection, Authorized Users should restrict use of the Internet to reputable websites that are known and trusted. The Agency reserves the right to moderate or restrict Internet traffic.

2C.3: Virus Protection and Encryption: Computers and devices connected to the Agency network must use encryption, have a virus protection application installed and be up to date with virus definition files. The IT Department will install these programs. Users shall not tamper with these programs.

2C.4: Report Known Issues & Suspected Concerns Immediately: Users must immediately report any known or suspected information security incident (such as virus/malware infection, data breach, or other system vulnerability) directly to the IT Department. IT shall treat such an incident as an **Emergency** matter (see 3B.2). Any concern regarding virus infection, data breach, or other circumstance in which an Authorized User's computer begins operating abnormally shall be reported to the IT Department immediately.

2C.5: Data Classification: Data stored on the Agency network in departmental shared folders should be classified in one of the three following categories:

Public: Information that is to be made available to the general public. Data in this category will be made accessible in a read-only format and should be stored on the "**X:\" drive**.

Restricted: Information that requires special precautions to protect from unauthorized use and is typically not to be disclosed to the general public, and potentially not to other departments. Any request for data of this type must first be approved by a Department Head. All data in this category should be stored on the "**Y:\" drive** in an appropriately named sub-folder.

Confidential: Information that is protected by law from use and/or disclosure shall not be provided to any requesting party without first receiving permission from legal counsel. This data shall be stored in permission-protected folders on the "**Y:\" drive, with access limited** to only those who need the information on a regular basis.

2C.6: Cloud-based Storage: The IT Department recognizes the value of Cloud-based storage solutions but only allows usage of select providers (e.g., Microsoft Government Cloud). Users shall not establish personal or departmental Cloud storage accounts with other providers.

2C.7: Data Release: Distribution of any data to a requesting party (internal to the Agency or an outside individual/entity), who is not otherwise authorized to directly access that data, must first be cleared by the Department Head who oversees the data.

2D. Remote Access

The IT Department understands the business need and value in offering remote access to Agency systems and networks. The authorized means of doing so are described below. Remote access is defined as accessing the Agency network by either an AOD or POD.

2D.1: Unregulated Remote Access: The IT Department allows users to access certain 'basic' Agency data and resources through standard web-services.

Prior Authorization Required	None
Usage Examples	Webmail, agency website, other web-based resources
Limitations & Restrictions	No limitation on AOD or POD

2D.2: Regulated Remote Access: For Authorized Users who require more functionality, the IT Department may provide the tools which allow for accessing specific applications or actual desktops remotely.

Prior Authorization Required	IT Setup
Usage Examples	Citrix (remote desktop / specific application access)
Limitations & Restrictions	No limitation on AOD or POD

2D.3: Native/Direct Access: For Authorized Users working with an AOD (such as a laptop computer) but need Agency network resources, Virtual Private Network (VPN) access can be setup. Vendors who need direct access to systems for maintenance tasks will be connected via a desktop support appliance.

Prior Authorization Required	Department Head & IT Director approval
Usage Examples	VPN (Authorized Users); Bomgar (Vendors)
Limitations & Restrictions	See policies below

2D.3A: Unless specifically authorized by the IT Department, only Agency Owned Devices (such as laptops) may be connected to the Agency VPN. If the computer connecting is not an AOD, it must be secured with a password that is not stored or remembered by the device or VPN connection.

2D.3B: Users take responsibility that no unauthorized user gains access to the computer or VPN connection.

2D.3C: Navigating or 'surfing' the web shall be limited strictly to work related topics & sites while connected to the VPN.

2D.3D: The computer with the VPN connection in place must have up-to-date virus protection/software.

2E. Loss, Theft, or Disposal of Equipment

2E.1: Immediate Reporting of Lost Devices: Authorized Users shall immediately report to their Department Head and the IT Department the loss or theft of any Agency Owned Device or Personally Owned Device with access to Agency systems.

2E.2: Reserved Right to Remote Wipe: IT reserves the right to delete the email box from or remote wipe any AOD or POD with access to Agency systems in the event of:

a. Loss or theft of device
b. Use by unauthorized user or former employee to access or store Agency data.

In such instances, the County will not be liable for any personal data that is lost in the process.

2E.3: Disposal Procedures: Prior to the disposal of any computer or device, IT staff shall remove all Agency data. Retired devices will be treated as e-waste and disposed of through recycling programs.

POLICY #3: SERVICE, STANDARDIZATION, AND PROCUREMENT

The IT Department provides support for all employees of Mono County and the Town of Mammoth Lakes, and handles all procurement of technology and software via a *Centralized Information Technology model*. The IT Department responds to support requests between 7am and 5:30pm Monday through Friday (excluding County holidays). After hours or on weekends & holidays, support requests may be opened for Emergency issues by emergency services or law enforcement agency staff, or any Department Head with an issue which cannot wait until the next business day due to a mission-critical support need. In these situations:

1. An IT technician will call back within two (2) hours of the initiated support request
2. An IT technician will attempt to work on the issue within 24 hours

3A. Technology Standards and Support Requests

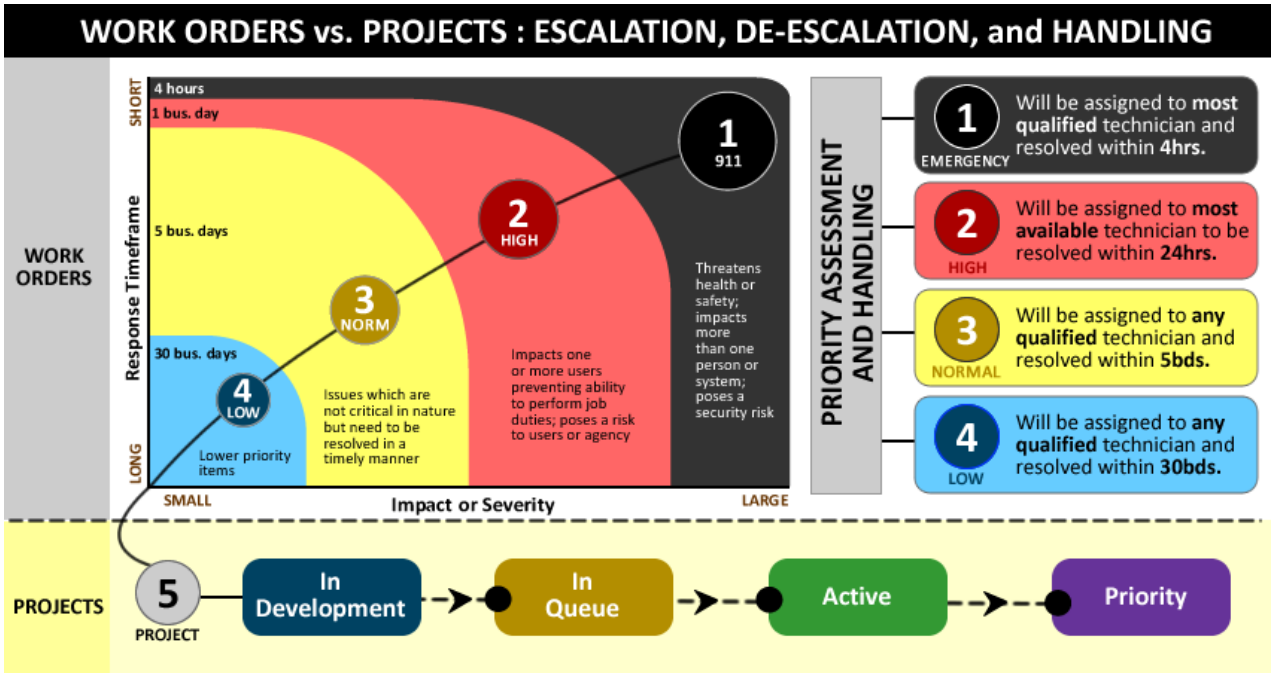
3A.1: Standardized Equipment: In order to provide quality support, the IT Department orders standard Windows-based PC computers and peripheral devices with which we have existing experience. For more information on procurement processes or standards, see Policy 3C.

3A.2: Tier 1 Support: IT Service is provided to all Authorized Users of Agency Owned equipment and for certain pieces of software and information systems for which there is no vendor support. Service shall not be performed by non-IT staff unless authorized in writing by the IT Department.

3A.3: Requests for Support: Requests for service shall be submitted to the IT Department through one of the following methods:

1. Email support@mono.ca.gov. Include in the subject line the nature of the support request and any provide additional information in the body of the message. This automatically generates a work order.
2. Call the IT Support Line at (760) 932-5500 (or x5500 from inside the County phone network) and follow the phone prompts to speak with a staff person or leave a message. Please call the IT Support Line for any **Emergency** or **High** Priority support issues.
3. 'Walk-in'—these must be entered into the queue before being worked and will be treated in the same manner as a phone or email request.

3A.3: Service Level Agreement: Requests The IT Service Level Agreement (SLA) gives priority consideration to Work Order tickets and other identified IT issues that affect more than one person, impact hard deadlines, or otherwise inhibit a User to perform his/her job.



*By default, all work orders are automatically classified as Normal unless otherwise specified or determined
Note: Purchasing requests are typically handled within three weeks (See Policy 3C)

3B. Procurement and Technology Replacements.

The IT Department is responsible for coordinating the purchase of all technology hardware and software. The IT Department recognizes that each department and User has unique and individual needs and will work closely with Department Heads and staff to ensure adequate equipment is procured.

3B.1: Purchase Requests: All technology purchases shall be placed only by IT staff. Department Head/Manager approval (with budgetary authority to make the technology purchase) is required before purchase is considered authorized. Purchase requests should include: (1) the business purpose of the intended purchase, (2) the account or fund that the charge can be made to, and (3) an official authorization to purchase.

3B.2: Maintenance and Upgrades: The IT Department exercises its best effort to keep computers in good working condition, and replace technology that is old or failing. Computers and technology installed within the Agency are of standard make and model, with rare and specific exceptions.

3B.3: Installations and Replacements: PC installations and replacements are handled automatically by IT staff on a three to five-year cycle pursuant to the IT Department's Infrastructure Replacement Program (IRP). IT will determine, purchase, and install machines appropriate for each User based on job demands.

a. PCs are required to be replaced when they reach 'end of life'. Prior to the beginning of each fiscal year, IT will review all PCs in service and provide Department Heads with an assessment of required PC replacements for the following year and the corresponding budget.

b. If a department uses grant funds to purchase PCs, they may choose to not 'enroll' a PC into the IRP. Instead, departments will be required to pay the actual invoice amount for each device being purchased that fiscal year.

ACCEPTANCE, COMPLIANCE, AND ADVERSE ACTION

The IT Standards and Policies are presented to Authorized Users at time of hire and are accepted prior to users being provided with Agency technology resources. Policies will be reviewed and updated on an annual basis and users will be presented with an Acceptance of Terms acknowledgement when logging on to Agency computers.

An Authorized User's acceptance of the IT Standards and Policies implies they are in agreement of and consent to:

a) Understanding and compliance of these Standards and Policies
b) Adhering to guidelines and recommendations pertaining to security
c) Complying with data management guidelines and directions
d) Protecting sensitive information against loss, unauthorized use/access, and disclosure
e) Using agency technology and information only for appropriate and approved purposes
f) Abiding by copyright and licensing laws for software and data
g) Reporting any known or suspected security incident or policy violation
h) Not engaging in any act which violates federal, state, or local laws, or policies set forth in this manual

It is each User's responsibility to immediately notify the IT Department of any known violations of this policy. Depending on the severity of the infraction, access to Agency resources may be wholly or partially restricted until a long-term remedy is put in place.

Failure to comply with this Policy Manual may result in disciplinary action up to and including termination of employment, in accordance with the applicable disciplinary rules of the County or Town.

EXCEPTIONS

Requests for exceptions to this Policy Manual must be reviewed by the ITSC and approved by the IT Director. The request must specifically state the scope of the exception along with justification for granting the exception, as well as the potential impact or risk.

POLICY MAINTENANCE

This policy manual is subject to review and modification on an annual basis (unless otherwise deemed necessary) by the ITSC.

DEFINITIONS

Agency Owned Device (AOD): These are mobile computing devices, including smartphones and tablets, which are purchased and owned by the County and issued to employees specifically for business or work purposes.

Business Use: Work-related responsibilities required by an employee's or an elected official's position.

Cellular Phone Costs: Identification of costs specifically associated with cell phone call expense and that a portion of such expense can be attributed specifically to County work and to the benefit and convenience of the furtherance of County use. Costs may be derived before the fact as within a committed cell phone use plan with a service provider, a 'cost per minute' plan or a 'pre-paid' by the minute plan.

Data Access Costs: Identification of costs specifically associated with Internet access expense and that a portion of such expense can be attributed specifically to County work and to the benefit and convenience of the furtherance of County use. Costs may be derived before the fact as within a committed Internet service plan with a data service provider, a 'cost per minute' or 'cost per bandwidth' plan or a 'pre-paid' by the time or bandwidth usage plan. The data service plan may or may not provide for a 'business' or 'enterprise' E-mail corporate access plan for access to the County Enterprise E-mail system.

Information Technology Steering Committee (ITSC): The Information Technology Steering Committee (ITSC) is a group of Department Heads, managers, and IT staff from the County and Town who help oversee and provide direction regarding the appropriate use of technology and information within the agencies. The ITSC helps to ensure that resources are used effectively within the organization in order to facilitate business operations and provide a positive experience for Users and constituents.

The ITSC assists with:

- Proposing and developing technology and information standards, policies, and guidelines
- Annually reviewing the Information and Technology Standards and Policies Manual
- Participating in strategic planning discussions about technology and information
- Bringing forward technology recommendations within core business areas relative to their subject matter expertise
- Providing input and feedback for organization-wide technology projects

Mobile Device: Device that provides an "always-on" end-to-end solution, combining hardware, software, and wireless connectivity, offering a complete email, messaging, organizer, Internet, and/or cellular phone solution. The device includes the adapter, battery pack and includes other equipment specific to the device used for County business purposes. A mobile device solution provides the ability to securely connect said device to the County's internal network and access County enterprise systems, technology, data, and information.

Personally Owned Device (POD): Also referred to as Bring Your Own Device (BYOD), these are mobile computing devices including smartphones and tablets which are owned by the employee and voluntarily utilized for work purposes.

Vendor: Any 3rd party contractor or consultant who sells goods and services to the Agency and is responsible for providing some level of support and assistance for those products.

APPENDIX I: AGENCY OWNED [MOBILE] DEVICES (AOD)

County departments may issue mobile devices for use with specific applications that support the mobile worker working in an outside environment. The mobile device may:

- Store agency data on directly on it;
- Connect back to the County network via a secured, remote connection;
- Connect to the Internet and access a Cloud supported service;
- Access County data internally or hosted in the Cloud.

A. Policies and Regulations:

Agency Owned Devices may be requested by Department Heads and issued to specific staff, or used as a shared device for a specific business need within a department.

- Use of any AOD is governed by Policy 1B as defined in the Information Technology Standards and Procedures.
- Assignment of or access to an AOD does not imply authorization for employee to work after hours or collect compensation for Over Time work which was not been pre-approved.

B. Department Head Responsibility:

Agency Owned Devices may be issued to employees for business use. Once issue, it is the responsibility of the employee and Department Head or Manager to ensure that:

- The devices are physically secured when not check out to an employee;
- Clear and complete use regulations, expectations, and impact thereof have been established, documented, and communicated to the employee before device has been distributed;
- Devices are properly logged when checked out and receiving back into physical custody of department;
- Department and its assigned user have agreed to maintain device in its originally configured state and that no additional applications, data, or connections will be added to the assigned device without authorization of the IT Department.

C. Employee Responsibility:

- Use mobile device only for the specific purpose as designated by his/her department;
- Use the device's Internet service on for supporting research as designated by the employees given responsibility as designated by the issuing department;
- Employee is responsible for the physical security of the issued mobile device;
- Follow recommended procedures to properly maintain the device's battery life;
- Employee is responsible for protecting the data, information, connectivity, and only uses the mobile device for its designated and authorized use;
- Employee is expected to abide by all state and federal laws governing use of device including those which prohibit use while operating vehicles, equipment, or otherwise create unsafe situations;
- Make the device available for updates, software patches, or other maintenance work that ensures the device remains current and secure;
- Employee must read, understand, and sign the Mobile Device User Agreement (Appendix A).

D. Joint Responsibility:

Both the employee and the department are ultimately responsible for informing the IT Department of any issue with the device, including but not limited to:

- Damage to or loss of device
- Appropriate use of device

E. Acceptance of Policy:

Employees are required to review and sign the Agency Owned Device User Agreement and adhere to the policies set forth in the Mono County PC Policies which govern use of AODs.

Mono County Agency Owned Device (AOD) Authorization

As a user of a County Agency Owned Device (AOD), I understand that I am to use this device only for County business and that I am required to follow the policies as set forth in the Mono County Information Technology Standards and Policies.

I acknowledge that it is solely my responsibility to understand the rules and requirements to participate in this program and if any issues arise, or assistance is needed with the AOD issued to me, or any item in the set of policies governing use of this device, I will immediately contact Mono County IT for clarification.

I have read and agree to comply with the Mono County Information Technology Standards and Policies related to use of an Agency Owned Device.

Name _____ Mobile Device Type _____

Office Phone _____ Mobile Device Number _____

Date Implemented _____

Comments _____

_____

_____

_____

Certification/Signature

Employee _____ Date _____

IT Approval _____ Date _____

Department Head _____ Date _____

Appendix II: Personally Owned Device (POD) /Bring Your Own Device (BYOD) STIPEND

Employees are permitted to use Personally Owned Devices (POD) for business or work purposes so long as they have been authorized to do so by their supervisor. If the Department Head determines that the use of a POD is required or necessary for performing their regular job and an AOD is not provided, the employee may be eligible for a stipend commensurate with the level and type of use of that employee's device.

A. Qualification Criteria
Department Heads shall consider the following criteria when determining qualification:

1. The nature of work assigned requires timely, business critical, two-way communication for which there is no reasonable alternative technology.

2. The employee provides emergency support and back-up from a mobile environment.

3. The necessity of a cellular phone or mobile device to insure the safety of the employee or others who may be at risk.

4. Need for the employee to immediately communicate with staff in the department and other agencies to coordinate programs or to provide adequate customer service for which a land line would not suffice.

5. The employee frequently works in the field where land lines and other primary radio or telephone communications are not available.

B. Use of Personally Owned Devices for business purposes

- The cellular phone is personally owned, and may therefore be used for both personal and business calls.
- Employees receiving a stipend must maintain an active cellular phone contract, with an add-on data plan (if necessary & approved), for the life of the allowance.
- Employees must provide their cellular phone numbers to the department, and agree to notify departments immediately of any changes to their cellular phone numbers or termination of their monthly service plans.
- There are no requirements to substantiate the business use of personally owned cellular phones. However, Department Heads may require employees to provide business usage documentation to validate the appropriateness of the monthly cellular phone allowance rates approved for the employees.
- Understanding that County information may be stored on certain devices, employees must follow basic security precautions, as outlined in Section 5C.
- Replacement or repair of the phone will be the responsibility of the employee who uses the phone.

C. Security for Personally Owned Devices

- If any agency data or information (including email or other records) are stored on the device, the employee must maintain a passcode on the device at all times.
- Device must be secured or in the possession of employee at all times.
- If an employee loses the device, the employee must immediately notify the Department Head and the Director of Information Technology.
- Device will not be altered (i.e.: 'Jail-broken') from its existing manufactured configuration and operating environment in an attempt to make device more flexible and/or more 'open' in accepting rouge applications and communications.
- Additionally, policies outlined in the Information Technology Standards and Policies Section 1C govern the use of Personally Owned Devices for business use.

D. Compensation

- The mobile device allowance is intended to cover the costs of personal mobile device cellular and data/Internet service expenses related to work duties.
- Initial purchase of the mobile device, accessory equipment, and activation fees and any long term contractual obligations will be the responsibility of the employee.
- The employee shall pay any costs exceeding the amount of the cellular phone and/or PDA allowance.
- No allowance will be paid when an employee is in an unpaid leave status or any other status except as an active employee.
- The County has established three tiers for the payment of monthly cellular phone allowance and a separate add-on allowance for e-mail and data service for PDAs based on anticipated or documented business usage.

Tier	Name	Definition	Payment
1	Limited Use Rate	This rate is appropriate for users with incidental or low usage level of up to 100 minutes per month	$25.00
2	Standard Rate	This rate is appropriate for users with usage level between 101 and 400 minutes per month	$35.00
3	High Use Rate	This rate is appropriate for users with anticipated or documented heavy volume usage of over 400 minutes per month.	$55.00
4	Data Add On	Applicable to employees using Personal Computing Devices (PCDs) such as smartphones or tablets with a data plan.	$50.00

- In exceptional cases, the County Administrator may approve a higher allowance for employees that demonstrate consistent documented official business use that exceeds the authorized allowance listed above. Occasional, infrequent spikes in business use do not qualify for a higher allowance or additional reimbursements.
- The Finance Director shall review the rates annually and recommend changes, as appropriate, to the existing rates to the County Administrative Officer for consideration.

E. Taxability

The mobile device allowance will be paid through the County payroll system as taxable income. For determination of individual's taxability, employees should check with their tax advisor.

F. Overtime

Overtime is strictly managed by your departmental policy and use of a mobile device after hours does not automatically confer permission to work overtime.

MONO COUNTY
PERSONALLY OWNED DEVICE STIPEND AUTHORIZATION

This form is to be completed when a County official or employee, as part of his or her job, needs to use a Personally-owned cellular phone/smartphone (or similar mobile device), or when that use is to be discontinued.

NOTE: Cellular Phones and devices with an activated service component may be Personally-owned or Agency-owned by an authorized official or employee. This form covers Personally Owned Devices (PODs) only. There is a separate agreement for Agency Owned Devices (AODs).

Employee: _____ Position: _____

Department: _____ Cell Phone #: _____

Type of Device: ☐ Cell Phone ☐ Smartphone ☐ Tablet/iPad

Amount Requested: $_____

A: ALLOWANCE FOR BUSINESS USE OF PERSONALLY OWNED DEVICE (POD)

Employee will provide his/her own cell phone/mobile device on _____ [date].

Employee will begin receiving an allowance within 30 days hereafter, and on a monthly basis, until he or she no longer needs to use the Cell Phone for County business purposes or chooses to stop this allowance.

The employee and his/her department head (for County elected officials or appointed department heads, the CAO) hereby certify that the employee needs to use a Cell Phone for County business because (initial all that apply):

Qualification Criteria	Employee	Dept. Head
1. The nature of work assigned requires timely, business critical, two-way communication for which there is no reasonable alternative technology.		
2. The employee provides emergency support and back-up from a mobile environment.		
3. A cellular phone or mobile device is needed to insure the safety of the employee or others who may be at risk.		
4. The employee must be able to immediately communicate with staff in the department and other agencies to coordinate programs or to provide adequate customer service, and using a land line would not adequately meet this need.		
5. The employee frequently works in the field where land lines and other primary radio or telephone communications are not available.		

COMPENSATION:

The supervisor of the requesting employee must initial all that apply:

Tier	Name	Definition	Payment	Approval
1	Limited Use Rate	This rate is appropriate for users with incidental or low usage level of up to 100 minutes per month	$25.00	
2	Standard Rate	This rate is appropriate for users with usage level between 101 and 400 minutes per month	$35.00	
3	High Use Rate	This rate is appropriate for users with anticipated or documented heavy volume usage of over 400 minutes per month.	$55.00	
4	Data Add On	Applicable to employees using Personal Computing Devices (PCDs) such as smartphones or tablets with a data plan.	$50.00	

TAXABILITY:

Any County official or employee accepting an allowance for a Cell Phone or for a cell phone service component of a PCD acknowledges that the allowance is considered to be taxable income by the Internal Revenue Service. For determination of individual taxability, officials and employees should check with their tax advisor.

DISTRIBUTION:

If this form authorizes an allowance, send the original of this form and a Personnel Action Form (PAF) to the Human Resources Department and keep copies of those documents in the department's files along with a copy of the service agreement or a current bill for service. If no allowance is being authorized, the department should keep the original of this form; no PAF, service agreement, or bill is necessary.

CERTIFICATIONS:

I certify that the foregoing is true and correct.

Date: _____ _____

Signature of Employee (or Official)

Date: _____ _____

Signature of Department Head (or CAO)