Policy Type	General Administrative Policy – Information Technology
Policy Name	D-02, Acceptable Use
Resolution Number	
Effective Date	November 12, 2024

PURPOSE

Appropriate organizational use of information and Information Technology (IT) resources, as well as the effective security of these resources, requires the participation and support of the County's workforce. Inappropriate use exposes the County to potential risks including malware attacks, compromise of network systems and services, and legal issues.

This policy applies to all workforce members, including employees, managers, Department Heads, and elected officials.

POLICY

SECTION 1: REQUIREMENTS

It is the responsibility of all to comply with this policy. Except for any privilege or confidentiality recognized by law, users have no legitimate expectation of privacy during any use of County resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed, or captured in any manner, including in real-time, and used or disclosed by authorized personnel without additional prior notice to users. IT may conduct periodic monitoring of systems used, including but not limited to: all computer files; all web browsing; and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems and other electronic records). The County may impose restrictions, at the discretion of their Department Head or the County Executive Officer, on the use of a particular resource.

A. Users accessing County applications and IT resources through personal devices must only do so with prior approval from both the appropriate Department Head and IT.

B. All users of information and information technology resources must comply with County policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including Federal, State, local and intellectual property laws.

C. Users must immediately report suspected information security incidents to their manager and the IT Help Desk at extension 6652 or by sending an email to security@calaverascounty.gov if the Help Desk is not available. This includes but is not limited to unauthorized disclosure involving County data and information.

D. Users must protect County resources, and information (e.g., personal, private, sensitive or confidential) from unauthorized use or disclosure.

E. Users must not distribute, transmit, post, or store any electronic communication, material, or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate.

F. Users must not attempt to represent the County in matters unrelated to official authorized job duties and responsibilities. Users must not connect unapproved devices to the County network or any IT resource.

G. Users must only connect to public Wi-Fi networks from sources they are familiar with, such as reputable hotels, conference centers, airports, or well-known coffee shops.

H. Users must avoid connecting to Wi-Fi networks from unfamiliar or untrusted sources, particularly those that cannot be verified as legitimate or that seem suspicious. Additionally, users must not connect to open Wi-Fi networks that do not require a password.

I. All activities conducted over public Wi-Fi must be securely connected to the County's Virtual Private Network (VPN). This ensures that sensitive data is encrypted and protected while being transmitted over potentially insecure networks.

J. Users must not connect to any wireless network while physically connected to the County's wired network.

K. Users must not download, install, or run software that has not been approved by IT.

L. Users must not access commercial email systems (e.g., Gmail, Hotmail, Yahoo, etc.) without prior approval from their department management and IT. Users must follow the County Email Policy at all times.

M. Users must not use County IT resources to circulate unauthorized solicitations or advertisement for non-County purposes including but not limited to religious, political, or not-for-profit entities.

N. Users must not use County information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions, etc.)

O. Users must not propagate chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using County resources.

P. Users must not tamper with, disengage, or otherwise circumvent County or third-party IT security controls.

Q. Users are prohibited from transmitting or storing any restricted, non-public, or confidential County information using personal email accounts (e.g., Gmail, Hotmail, Yahoo) or unapproved third-party storage services (e.g., Dropbox, Box, etc.). This includes conducting County business through personal email accounts. Additionally, storing such sensitive County information on devices not issued by the County is not permitted, unless the device or storage service has received prior approval from IT. Any device accessing County data including email must have a passcode or password to prevent unauthorized access.

R. Unless specifically authorized, the use of County email addresses on public social media sites is prohibited.

S. Users must not execute any form of network monitoring, packet capture, port scan, security scan, or vulnerability scan unless performed within the user's official job duties.

T. Users must not reveal or share their account password(s) with anyone or allow others use of their account. IT will never ask a user for their password. If anyone insists that they be provided with one or more of your passwords, notify the IT Director or Human Resources Director.

U. County resources, such as computers, mobile devices, and network systems, must not be used or accessed by family members or any unauthorized individuals for personal, non-County related activities, including but not limited to schoolwork or personal tasks.

SECTION 2: OCCASIONAL AND INCIDENTAL PERSONAL USE

Occasional and incidental personal use of IT resources is permitted, provided such use is otherwise consistent with this policy as long as the use is not contradictory to departmental policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill the County's responsibilities and duties, including but not limited to, excessive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important. At the discretion of the Department Head or County Executive Officer, the County may revoke or limit this privilege at any time.

SECTION 3: INDIVIDUAL ACCOUNTABILITY

Individual accountability is required when accessing all IT resources and County information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking computer screens when walking away from workstations, and protecting credentials (e.g., passwords, tokens or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information and must not be disclosed or shared.

COUNTY OF CALAVERAS
ADMINISTRATIVE POLICY

Policy Type	General Administrative Policy – Information Technology
Policy Name	D-03, Artificial Intelligence
Resolution Number	
Effective Date	November 12, 2024

PURPOSE

The purpose of this Artificial Intelligence (AI) Usage Policy is to establish guidelines and best practices for the responsible use of AI systems within the County. The policy aims to promote the efficient and ethical use of AI tools while minimizing the risk of intentional or unintentional misuse that may result in harm to individuals, the organization, or our mission.

Given the rapid and transformative growth of AI technologies, this policy acknowledges that the use of AI is expanding at an unprecedented pace. Consequently, the policy may be updated as necessary to adapt to emerging AI trends and challenges. Furthermore, internal AI workgroups may be established as needed to evaluate and determine the appropriate and valid uses of AI within the organization.

POLICY

SECTION 1: REQUIREMENTS

It is the responsibility of all users to ensure they are in compliance with this policy.

A. Users must adhere to all County policies, procedures, rules, and regulations, particularly those related to regulatory requirements, information security, and technology. Collected, stored, processed, or accessed data must be protected accordingly.

B. Users must exercise due diligence and critical thinking when using AI-generated outputs, as AI systems may produce biased, inaccurate, or inappropriate results.

C. Users must review AI-generated outputs for common biases present in AI systems, such as data bias, algorithmic bias, and confirmation bias.

D. Users must verify the accuracy of AI-generated outputs through cross-checking with reliable sources, human judgment, or other relevant methods. Users must ensure that a human properly reviews and approves AI-generated content for use.

E. AI-generated outputs must be assessed for appropriateness, considering the context, audience, and potential impact of the content.

F. Department Heads or managers must approve the use of AI-generated content within their department or functional area. Implementing guidelines to ensure appropriate AI tool usage is strongly recommended.

G. Users must ensure that sensitive and personal data is anonymized or otherwise protected when used with AI tools.

H. Sensitive data must never be input into an AI tool unless an appropriate agreement exists between the vendor and the County, and all necessary safeguards are in place to protect sensitive data. Sensitive data must never be used in online generative AI tools (e.g., ChatGPT, Microsoft Copilot, Bing, etc.)

I. Users must promptly report data breaches, whether intentional or unintentional, to IT. If the breach involves HIPAA protected data, the designated HIPAA Compliance Officer must also be notified. Providing protected data (e.g., PII, ePHI, etc.) to an unapproved AI tool will be considered a potential breach.

J. Users must not misuse AI tools, either intentionally or unintentionally. Misuse includes, but is not limited to, AI-based fraud, discrimination, social engineering, spreading misinformation, privacy violations, inaccurate or misleading information, and inappropriate content.

K. All software and vendor services containing or utilizing AI must be thoroughly vetted by the County IT Department prior to purchase, implementation, or integration into any County systems or workflows.

History:

Policy Type	General Administrative Policy – Information Technology
Policy Name	D-05, Email
Resolution Number	
Effective Date	November 12, 2024

PURPOSE

This policy outlines the proper use of email resources available to users to ensure that County provided email services are used in compliance with applicable laws and County policies. Users who use email services must familiarize themselves with this policy. By complying with this policy, Users can ensure that disruptions to the County's email services are minimal and that the County can continue to manage email in an efficient manner.

POLICY

Email is a means of transmitting messages and other digital communications electronically. The purpose of email is to communicate between individuals and groups and to promote the effective and efficient use of time and resources to carry out County business. Only County provided email accounts shall be used to conduct County business.

SECTION 1: REQUIREMENTS

It is the responsibility of all users to ensure they are in compliance with this policy.

A. Email messages sent and received on the County email system are intended to support communication internally and externally that is reasonably associated with the needs of the County. Email is always considered to be Public Record. Users shall have no right or expectation of privacy in any email message drafted, sent, or received on the County's email system and the County reserves the right to read all such email messages.

B. Department Heads may be granted access to review any email message sent or received on the County email system by any user supervised by their department after making a request in writing to Information Technology (IT) and receiving approval by the Human Resources Director.

C. Misuse of email brought to the attention of IT may be reported to an individual's Department Head or Human Resources. For more detailed information about these types of misuse, refer to Section 3 of this policy - Inappropriate Email Use.

SECTION 2: USE OF THIRD-PARTY EMAIL

A. Use of third-party email services, such as Gmail or Yahoo mail, including forwarding of County email to such third-party email services to conduct County business, is prohibited. If a County user receives email on a third-party email service and a response to the email is required, the user will forward the email to their County email account and reply from the user's County email with instruction to the original sender that future correspondence should be sent to the County email address.

SECTION 3: EMAIL SECURITY

A. Email and Network authentication methods (e.g., passwords, tokens, devices etc.) must not be shared with anyone. Access to user accounts must be limited to the account owner.

B. In the event that a user is required to view another's email as part of his or her job duties, that user may be granted permission to access the email via a proxy following a request to the IT Director from the Department Head of the user whose email is to be viewed. Permission may be granted to view and if required, send email on behalf of another's email. No user will be granted rights to send mail "as" the other user (impersonation).

C. Every user will participate in ongoing training related to Security Awareness, recognizing phishing, and steps to protect the County network and computers.

D. Users shall treat all email with suspicion and look for red flags taught in Security Awareness Training, particularly those emails containing links, attachments, or requests for the user to provide professional or personal account information or take some type of action that is not in line with normal County business activity.

E. Users shall report to IT email that is determined to be suspicious or potentially harmful by using the button in Outlook for reporting phishing messages or by forwarding the message to suspicious@calaverascounty.gov.

F. Email with content or attachments containing sensitive or protected information that is sent to external address(es) must be sent in a manner consistent with County procedures for sending secure email.

SECTION 4: APPROPRIATE EMAIL USE

Appropriate use of email includes:

A. Email used to conduct valid business-related communications that do not violate established County policies.

B. General communications within the scope of the sender's job responsibilities.

C. Informational announcements being communicated to County Workforce Members.

D. Transmission of files as email attachments. Note that email attachments have size limitations. If the total size of a message exceeds the allowable limit for email transmission, contact IT for alternative methods to send the file(s).

SECTION 5: INAPPROPRIATE EMAIL USE

Inappropriate use of email includes, but is not limited to the following:

A. Transmitting Protected Health Information (PHI) in a manner that is inappropriate and/or violates HIPAA and/or State or County level regulations protecting PHI.

B. Sending information with malicious intent that may be damaging to the County, its Workforce Members, the public, or individuals or entities not directly associated with County business.

C. Distributing any material or comment that is discriminatory, offensive, defamatory, or harassing.

D. Engaging in the promotion of or participation in illegal activities.

E. Disseminating copyright infringing materials.

F. Sending items having to do with political activities not related to County business.

G. Engaging in personal attacks on other County staff or external individuals.

H. Creating or forwarding monetary recruitments of any type.

I. Using County email for any non-work-related personal website or list registration using County email ID.

J. Using County email to forward sensitive, protected, or confidential information to an external entity for non-County business purposes.

K. Misrepresenting an employee's identity.

SECTION 6: ACCESS OF EMAIL

Email may be accessed through various methods.

A. The majority of County email is accessed by users at an approved work location via a County provided computer that is connected to the County network. Access is provided based on a request made by the Department Head.

B. Approved Mobile devices (iPhone, Android phone, iPad, etc.) may connect to the County email system. The user's network ID and password may be stored on the device. Mobile devices that connect with County email must have passcode or password locks in place on the device. The user's Department Head must sign off on requests for a user to access email on a mobile device.

C. Webmail: A user may access County email through the internet by using Webmail. The user will need to provide County network ID and password as well as use multi-factor authentication when using Webmail.

D. Personally owned devices connecting to County email may be subject to public records requests.

SECTION 7: EMAIL RETENTION PERIOD

Length of time that email is retained by the County's email management system and by the County's email archival system.

A. Email is retained in the County's email management system. The user accesses and manages their email through Microsoft Outlook, the Outlook Mobile App, or Outlook Webmail. The user can retain or delete email in Outlook.

B. Email retained and managed within the Inbox folder, Sent folder, Deleted items folder, and all subfolders nested within these folders, will be purged by the system two years and one day after the email was received or sent. The user's email system will work more efficiently with smaller total volumes of email in the user's email folders.

C. All email that is sent or received, will have a copy of the email saved in an email archive system. The user can search for and retrieve archived copies of email for their account. The user has no ability to update or delete the original copy of the archived email but can reply to or forward archived email. Copies of email saved to the email archive system will be purged by the system two years and one day after the copy of the email was saved to the email archive system.

D. Users are advised against using separate archive or data files in the PST format or other mechanisms to create electronic copies of email files. These mechanisms are not as reliable as the County's main email system and email archive system and will not be supported by IT.

SECTION 8: PUBLIC RECORDS

A. Any information transmitted by e-mail that meets the definition of "public record" under the California Public Records Act may be subject to public records requests.

B. All email related public record requests will use the County email archival system as the County's official record for archived copies of all email sent and received for the most recent two-year period.

C. All email public record requests will be provided to County Counsel. County Counsel will review requests and manage internal processes to retrieve archived copies of email, make determinations on applicability of email as a public record and communicate results to the requesting party.

SECTION 9: LITIGATION HOLD

A. Email may be subject to orders to hold archived email for longer than standard archival retention period.

B. Email may be subject to requirements to preserve archived records for pending or reasonably anticipated litigation. When a litigation hold is required, County Counsel will provide criteria that IT will use to retain archived copy of email for a period defined by County Counsel.

C. All email that meets the definition of litigation hold email, will use the County email archival system as the County's official record for litigation hold archived copies of email.

D. County Counsel will manage internal processes to retrieve litigation hold archived copies of email as necessary to support requests to provide litigation hold email.

E. When County Counsel determines that a litigation hold is no longer required, County Counsel will notify IT staff in writing. IT will then remove the litigation hold and all previously held email will then be subject to standard retention periods.

COUNTY OF CALAVERAS
ADMINISTRATIVE POLICY

Policy Type	General Administrative Policy – Information Technology
Policy Name	D-07, Mobile Device
Resolution Number	
Effective Date	November 12, 2024

PURPOSE

The County is tasked with protecting the confidentiality, integrity, and availability of data. Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other devices that are only used within the County's facilities and on the County's networks. The purpose of this policy is to establish the protections required for mobile devices.

POLICY

SECTION 1: REQUIREMENTS

Requirements of this policy for the protection of County assets including information are defined below. It is the responsibility of all users to ensure they are in compliance with this policy.

A. Mobile devices are computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and are portable (i.e., non-stationary). These devices come in many forms such as: smartphones, smartwatches, tablets, laptops, and wearable devices. Mobile devices must follow all applicable requirements in all County information security policies.

B. All users must assist in protecting devices issued by the County or storing County data.

C. Users are expressly forbidden from storing County data on devices that are not issued by the County without written approval from the Department Head and Information Technology (IT) Director. In cases where this is approved, the authorized user will sign an agreement stating they will abide by all security policies and procedures.

D. All mobile devices that access or contain County information must be encrypted. For mobile phones and tablets, this often includes having a minimum six-digit passcode to unlock the device.

E. Users are to notify IT immediately if they see error messages pertaining to endpoint protection or software updates for these products.

F. Only approved applications may be installed on County issued mobile devices. Applications must be digitally signed to ensure that only applications from trusted entities are installed on the device and that code has not been modified.

G. Mobile devices not issued by the County must not have direct access to County managed networks. This does not apply to authorized email and calendar access through the web.

H. County information must be removed or rendered inaccessible from mobile devices after no more than 10 incorrect authentication attempts.

I. Mobile devices must automatically lock after being idle for a period not to exceed 10 minutes. Requirements may be more stringent for some functional areas based on the types of data in device email or accessible by the device.

J. Mobile devices which directly connect to managed private networks, virtually connect to managed private networks in a manner consistent with a directly connected device, or which contain or could contain information, including e-mail data, must be managed by the County Mobile Device Management (MDM) solution.

K. Use of synchronization services, such as backups, for mobile devices (e.g., local device synchronization, remote synchronization services, and websites) must be controlled through an MDM or other centralized management solution.

History:

L. Mobile devices may not access private networks unless their operating environment integrity is verified (including whether the device has been rooted/jailbroken).

M. County issued mobile devices that access, process, or store County information must be procured through IT and managed through the IT MDM system.

N. County IT must manage all mobile devices by:

1. Implementing device policies and configurations as appropriate to the use of the device.
2. Developing and implementing processes which check for upgrades and patches to the software components, and for appropriately acquiring, testing, and deploying the updates to entity issued devices.
3. Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.
4. Detecting and documenting anomalies which may indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.
5. Providing training and awareness activities for mobile device users on threats and recommended security practices which can be incorporated into the entity's security and awareness training.

History:

Policy Type	General Administrative Policy – Information Technology
Policy Name	D-09, Remote Access
Resolution Number	
Effective Date	November 12, 2024

PURPOSE

The purpose of this policy is to establish authorized methods for remotely accessing County network resources and services securely from a computer, laptop, or similar device.

Major security concerns arise with remote access including the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, the availability of internal resources to external clients, potential damage to resources, and unauthorized access to information. The requirements below are designed to minimize the potential exposure to damage resulting from the loss of confidentiality, integrity, or availability of sensitive or mission critical data.

POLICY

SECTION 1: REQUIREMENTS

It is the responsibility of all users to ensure they are in compliance with this policy.

A. Users agree that they are subject to the same County policies, procedures, rules, and regulations that apply when they are working on-site, in particular, those related to regulatory requirements, information security, and technology. Data collected, stored, processed, or accessed must be protected accordingly.

B. Authorized users must:

   1. Maintain security awareness at all times and must notify their supervisor and the County Information Technology (IT) division in the event of an actual or suspected security incident.
   2. Not introduce a malicious program into a County device or the County network willfully, or through negligence.
   3. Protect their login and password from unauthorized disclosure to anyone else including family members and adhere to the County's Password and Authentication Policy
   4. Complete County Security Awareness Training and be signed off by IT as being eligible for remote access.

C. Remote connections to the County network require users to:

   1. Use a County-issued device (e.g. laptop, tablet, mobile phone, etc.). Personal devices are not allowed unless the device, specification, and configuration are approved as an exception by the authorized User's Department Head and the IT Director.
   2. Ensure that any external network being connected to is provided by a trustworthy source.
   3. Use an encrypted Virtual Private Network (VPN) Tunnel provided by the County secured by using Multi-Factor Authentication (MFA)
   4. Limit activity to County business if using public WiFi (e.g. coffee shop, restaurant, airport, hotel, etc.)
   5. Take steps to safeguard sensitive data from unauthorized disclosure when it may be visible to those around them. This may include the use of a privacy filter for the screen.
   6. Lock their screen when stepping away just as they are expected to do when working in the office.
   7. Disconnect from the County network including the VPN connection when not actively performing work for a period of time exceeding 60 minutes or at the end of the workday.

D. County approved devices must:

   1. Have an approved version of a vendor-supported operating system.

2. Have an approved version of a vendor supported anti-virus and/or endpoint protection solution with an active subscription.
3. Have registered a full anti-virus scan within the last thirty days or have an approved next generation endpoint protection solution that provides continuous active protection.
4. Be up to date with all vendor security patches and updates current within 30 days.
5. Pass a basic health check to ensure the client meets the requirements in the Acceptable Use. The basic health check requires the systemic collection of data from the device connecting to the network. Data collected will typically include device hardware information, operating system, security and antivirus protection, installed software, and configuration.

E. Users will not use personal accounts to transmit County data or transfer data between work locations, including personal email, personally owned storage devices (thumb drives, etc.) or personal cloud storage accounts.

F. Storage and transfer of County data must be performed only through County approved methods, which include County-provided drives and County-approved cloud storage services.

G. County cloud resources (e.g., Microsoft 365, etc.) must not be accessed from a personally owned device.

H. For security and network maintenance purposes, IT staff may monitor and/or audit County-issued equipment, systems, and network traffic at any time.

I. Access to the County network will be limited based on the principle of "least privilege"

History: