SUBJECT: ACCEPTABLE USE POLICY

I. PURPOSE:

The Technology Services Department is committed to protecting Douglas County's employees, partners and the County organization from illegal or damaging actions by individuals, whether done knowingly or unknowingly.

Information resources are strategic assets of Douglas County and must be treated and managed as valuable resources. The purpose of this policy is to do the following:

A. Establish minimum appropriate and acceptable requirements regarding the use of information resources connected to the County Network.

B. Comply with applicable County laws and other rules and regulations regarding the management of information resources.

C. Provide clear guidance to those individuals who may use information resources with respect to their responsibilities associated with computer resources.

D. Establish a process to ensure that users acknowledge their agreement to comply with the rules of behavior before gaining access to information resources connected to the County Network

II. SCOPE:

This policy applies to the use of electronic information, computing devices, and network resources used to conduct Douglas County business or interact with internal networks and business systems, whether owned or leased by the County, the employee, or a third party.

This policy applies to all Users of the above-described resources. Users are defined as employees, contractors, consultants, temporary hires, and other workers at Douglas County, including all personnel affiliated with third parties.

III. GENERAL ACCEPTABLE USE POLICY:

A. Users may not connect personal devices to the County Network without express approval from the Technology Services Department. This requirement does not apply to users who connect to the County Network through a county-supplied "guest" Wi-Fi network.

B. Personally owned "smart" devices may not be connected to the County Network without pre-approval. "Smart" devices, commonly referred to as the "Internet of Things," includes such devices as thermostats, wearable technologies, non-stipend smart phones, or other appliances.

C. All authorized devices connected to the County Network must have updated malware/anti-virus protection.

D. Users must not attempt to access any data, documents, email correspondence, or programs contained on systems for which they do not have authorization.

E. County employees and other County Network users shall not access or attempt to gain access to any computer account for which they are not authorized to access.

F. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.

G. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or other similar information or devices used for identification and authorization purposes.

H. System level and user level passwords must comply with Douglas County's Password Policy.

I. Users must not make unauthorized copies of copyright protected or County-owned software.

J. Users must ensure all files downloaded from an external source to the County Network or any device connected to the County Network, including a diskette, compact disc (CD), USB flash drive, or any other electronic medium, is scanned for malicious software such as viruses, Trojan horses, worms or other malicious code.

K. Users must ensure that the transmission or handling of personally identifiable information (PII) or other sensitive data is encrypted or has adequate protection.

L. Users may not download, install or distribute software to County-owned devices unless it has been approved by the Chief Technology Officer or their designee.

M. Users must not download County data to personally owned devices unless approved by the Department Director or their designee.

N. Users must not purposely engage in activity that is illegal according to County, state or federal law, or in any activity that may harass, threaten or abuse others, or intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene. Such activity includes, but is not limited to, the following:

   i. Using a Douglas County computing asset to actively engage in procuring or transmitting material that is sexual in nature and/or is in violation of sexual harassment or hostile workplace laws. Employees authorized to conduct investigations are exempt from this provision when acting within the scope of their investigation.

   ii. Using email, the Internet, or the Intranet to harass or intimidate another person, such as broadcasting unsolicited messages or sending unwanted mail, is expressly prohibited. Employees using email or the Internet to harass or intimidate another person are subject to disciplinary action, including termination.

   iii. Using email, the Internet, or the Intranet to send or receive sexually explicit and/or sexually harassing content, whether implied or expressed, is prohibited. Employees using

email to send sexually harassing content, whether implied or expressed, or to view, download or access sexually explicit and/or sexually harassing content, whether implied or expressed, are subject to disciplinary action, including termination. Employees authorized to conduct investigations are exempt from this provision when acting within the scope of their investigation.

O. Users accessing the County Network must avoid unnecessary network traffic and interference with other users. Specific prohibitions include, but are not limited to, the following:

   i. Unsolicited commercial advertising by public employees and County Network users. For the purpose of this policy, "unsolicited commercial advertising" includes any transmission initiated by a vendor, provider, retailer, or manufacturer of goods, products, or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer that describes goods, products, or services.

   ii. Any other type of mass mailing by employees and others accessing the County Network that does not pertain to governmental business or a County-sponsored activity.

   iii. Streaming audio or video files that are not related to one's job duties and responsibilities.

P. Users must not engage in activity that may degrade the performance of information resources, deprive an authorized user access to resources, obtain extra resources beyond those allocated, or circumvent information security measures.

Q. Users must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of information technology resources unless approved in writing by the Chief Technology Officer or their designee.

R. Information technology resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any state, County or federal law.

S. Access to the Internet from County-owned, home based, devices must adhere to all acceptable use policies. Employees must not allow family members or other non-employees to access non-publicly accessible information systems.

IV. EMAIL AND INTERNET ACCEPTABLE USE POLICY:

A. All communications sent or received by County email systems and/or email communications on County business in personal email accounts may be subject to public records laws and eDiscovery requests and shall be managed according to the requirements of the County's record

retention policy. Employees must act with concern for laws regulating public records access and the subpoena of computers and records.

B. Personal email accounts are not to be used to send and receive official County correspondence and are not to be configured on County computers and devices.

C. County personnel shall exercise due care when addressing email correspondence to ensure that the correspondence is addressed correctly and that the intended recipient is authorized to view content within emails or documents. Examples of email content that constitute unacceptable use include the following:

   i. Private or personal for-profit activities. This includes personal use of email for marketing or business transactions, advertising of products or services or any other activity intended to foster personal gain.

   ii. Unauthorized not-for-profit business activities.

   iii. Seeking/exchanging information, software, etc., that is not related to one's job duties and responsibilities.

   iv. Unauthorized distribution of County data and information including the unauthorized use of email auto-forwarding.

   v. Use for, or in support of, unlawful or prohibited activities as defined by Federal, State and County laws or regulations.

D. Prohibited activities relating to Internet and network access include the following:

   i. Tampering with computer hardware or software.

   ii. Knowingly vandalizing or destroying computer files.

   iii. Transmitting threatening, obscene or harassing materials.

   iv. Attempting to access a remote site/computer without proper authorization.

   v. Using the Internet to access data that is protected and not intended for public access.

   vi. Violating Federal and State laws dealing with copyright protected materials or materials protected by a trade secret.

   vii. Sending confidential information without encrypting that information, thereby exposing the data to discovery by unintended recipients.

   viii. Intentionally seeking information about, obtaining copies of, or modifying contents of files or data belonging to other users, unless explicitly authorized to do so by those users.

ix. Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by network administrators. Assisting others in violating these standards by sharing information or passwords is also unacceptable behavior.

x. Deliberate interference or disruption of another user's work or system. Users must not take actions that cause interference to the network or cause interference with the work of others on the network. Users are prohibited from performing any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of system/network performance) or the introduction of computer worms, viruses or other malicious software/hardware by any means.

E. Misdirected or unsolicited email shall be treated with caution. Recipients shall not open or respond to unsolicited email. Potential security risks are involved in responding to unsolicited commercial email (spam), including responding to an invitation contained in such email to have one's email address removed from the sender's list.

F. Douglas County employees shall use due care when forwarding messages so that users do not do the following:

i. Auto-forward email without first obtaining department approval.

ii. Knowingly send out an email message that contains viruses, Trojan horses or other malware.

iii. Use the electronic-mail system or network resources to propagate chain letters, misinformation, or hoax information.

iv. Forward any confidential information to any party without the prior approval of a local department manager.

v. Forward any confidential information without appropriate protections such as encryption.

vi. Send information or files that can cause damage to the County or its citizens.

vii. Send unsolicited messages to large groups of people except as required to conduct County business.

G. Technology Services shall provide notifications and/or training on the security issues involved in receiving email to ensure that employees are aware of potential problems that can be introduced into the network and how to avoid them.

H. County employees shall protect County resources by not acting on unsolicited and commercial electronic mail such as:

i. Activating or clicking on hyperlinks in documents or email messages that are from unknown sources or part of unsolicited messages (spam).

ii. Responding to or following hyperlinks asking for usernames and passwords when asked to do so by unsolicited phishing emails.

I. Email and Internet services are provided primarily to conduct official County business. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of County-provided email, Internet, and Intranet.

J. While performing work-related functions or while using publicly owned/publicly provided information-processing resources, including mobile devices, County employees and authorized users shall use network resources and the Internet responsibly.

K. Users accessing the County Network shall do the following:

i. Ensure that there is no intentional use of such services in an illegal, malicious, or obscene manner.

ii. Ensure that all applicable software copyright and licensing laws are followed.

iii. Guard against wasting County Network resources, such as excessive personal use.

iv. Avoid using Internet streaming sites except as consistent with the mission of the County and for the minimum amount of time necessary to obtain the desired amount of information.

v. Not take actions that would constitute a criminal offense or make the County liable to civil suits, such as stalking, or actions that are abusive, fraudulent, hateful, defamatory, obscene or pornographic in content.

vi. Not access or attempt to gain access to any computer account or network that they are not authorized to access.

vii. Users of Internet search engines shall take precautions when using Internet search engines to verify the integrity of the information provided by the search engine. As users collect information gathered from the Internet, they must do the following:

1. Check data for their integrity and accuracy before using them for business purposes.

2. Observe all copyrights, end user licensing agreements, and other property rights.

V. COMMUNICATION DEVICES

Communication devices, including all mobile devices such as cellular telephones, smart phones, and tablets, are provided by the County with the intent to allow an employee to conduct official County business more efficiently.

The policy covers all personnel to whom these devices are issued for conducting their County business as well as those employees charged with the administration and maintenance of this equipment.

A. Employees are responsible for exercising good judgment regarding personal use of all communication devices, including office telephones and fax machines, and other County-provided devices.

B. If it has been determined by the Elected Official or department head, on a case-by-case basis, that an employee needs to have a mobile device for County business purposes, the employee may choose to receive a County-owned mobile device and adhere to all required audit and use procedures detailed in this policy or may elect to receive a stipend from the County (as detailed in County Policy 100.29) for the usage of their personal mobile device for County business purposes.

C. Employees are prohibited from downloading and installing unapproved and unauthorized software applications on County mobile devices.

D. Upon activation, Technology Services Department personnel will install anti- virus, security software, and/or encryption onto each communication device, as applicable. Employees must not un-install or de-activate any anti-virus or security software loaded onto the communication device or perform any other activity that defeats any process to update virus signatures or other security systems installed by the Technology Services Department.

E. Employees may not connect, dock or otherwise synchronize any County mobile device with any privately-owned or non-County computer, laptop, server, system or network, without the prior consent of the Information Technology (IT) Manager, or their designee.

F. The Technology Services Department reserves the right to refuse network connection for any communication device when not in compliance with this policy. The network connection will be re-enabled only after the Technology Services Department verifies the security status to be in compliance.

G. Employees provided with County mobile devices are responsible for the safe keeping of those devices. Employees are to keep the devices on their person at all times when traveling. Employees are responsible for replacing damaged, lost, or stolen mobile devices.

H. In the event a County mobile device is lost, stolen or misplaced, the Technology Services Service Desk should be notified immediately (regardless of time of day) so that appropriate steps can be taken to remotely trigger the timely deletion of all sensitive, proprietary or confidential information contained on the mobile device.

I. Electronic communications are not private or confidential. Any information located on a County communication device is the property of Douglas County and may be considered a public record. There are no rights to individual privacy on a County communication device. Any confidential, personal information located on the communications device could be considered public record and disclosed to third parties.

J. It is the responsibility of the Elected Official, department head, manager, and/or supervisor to monitor their department's phone and data services usage and the ongoing cost of those services and take appropriate action to remedy any misuse of a communication device by their employees.

K. The Technology Services Department may, on occasion, audit phone and data service usage, without notice to the department or employee, to ensure appropriate usage plans are selected.

L. The Technology Services Department shall establish the rate plan for mobile device service based on the most economical plan for usage history. An Elected Official or department head may request a plan upgrade or downgrade.

M. The Technology Services Department is only responsible for identifying compatible platforms, purchasing equipment, and supporting County mobile devices. The Communications Division is not responsible for determining employee eligibility or allocating funds to pay for mobile devices, accessories and/or service fees. The requesting Elected Official, department head, manager, or supervisor must allocate funds from their department's operating budget to cover costs arising from the mobile device request.

VI. AUDIT:

A. It is the responsibility of Supervisors, Department Heads, Elected Officials, or their designees to monitor their department's e-mail and Internet usage. Employees from the Technology Services Department may, on occasion, audit e-mail and Internet usage, with notice given to the Supervisor, Department Head, Elected Official, or their designee, to ensure proper use of the e-mail and Internet systems.

B. It is the policy of Douglas County NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored, and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their

electronic communications in recognition of the fact that the County will from time to time examine the content of electronic communications. Elected Officials and Department Heads or their designees may examine e-mail at any time.

C. Consistent with generally accepted business practice, Douglas County may collect statistical data about electronic communications. Using such information, Technology Services Department staff shall monitor the use of the Internet and electronic messaging to ensure the ongoing availability and reliability of these systems. Supervisors, Department Heads, Elected Officials or their designees may request copies of statistical data reports from Chief Technology Officer at any time to ensure compliance with this policy.

D. At any time and without prior notice, Human Resources, in coordination with the District Attorney's Office, reserves the right to examine e-mail, personal file directories, and other information stored on Douglas County computers. This examination assures compliance with internal policies; supports the performance of internal investigations; and assists with the management of Douglas County information systems.

VII. REPORTING SECURITY PROBLEMS:

A. If sensitive County information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the employee's Supervisor, Department Head, Elected Official, or their designee shall be notified immediately. Subsequently, the Supervisor, Department Head, Elected Official, or their designee shall notify the Chief Technology Officer, or their designee, immediately.

B. If any unauthorized use of Douglas County's information systems has taken place, or is suspected of taking place, the Chief Technology Officer, or their designee, shall be notified immediately.

C. Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like shall also be immediately reported to the Chief Technology Officer, or their designee.

D. Users must report any incidents of possible misuse or violation of the Acceptable Use Policy.

VIII. COMPLIANCE VERIFICATION:

The Chief Technology Officer, or their designee, will verify compliance with this policy through various methods including, but not limited to, business tools and reports, and internal and external audits.

IX. NON-COMPLIANCE:

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Email and Internet access, and the use of County-provided technological devices, may be revoked at any time by the County Manager, Elected Official, or Department Head.

X. **EXCEPTIONS:**
Any exception to the policy must be approved by the Technology Services Security team in advance.

The Douglas County Courts maintain its own technology, network, and servers, and is hereby exempt from compliance with the Acceptable Use Policy. County employees who operate on and use the Court's network or technology devices shall comply with the Court's established policies. Violation of those policies may result in disciplinary action, up to and including termination of employment.

XI. **RESPONSIBILITY FOR REVIEW:**
The Internal Review Committee shall review this policy as needed or at least once every 3 years.