CAMERON COUNTY

END USER COMPLIANCE POLICY

Revised

April 2018

Approved by Commissioners' Court

Date: _____

Contents

I. POLICY AND PURPOSE STATEMENT 1
II. AUTHORITY 1
III. DEFINITIONS 1
IV. USER ROLES AND RESPONSIBILITIES 2
V. PHYSICAL AND ENVIRONMENTAL SECURITY 4
VI. PASSWORD MANAGEMENT 4
VII. E-MAIL 5
VIII. NETWORK AND INTERNET/INTRANET 8
IX. SOCIAL MEDIA 11
X. COMPUTER SOFTWARE USAGE, MAINTENANCE, AND EQUIPMENT 13
REFERENCES 15

END USER COMPLIANCE POLICY

POLICIES AND PROCEDURES

I. POLICY AND PURPOSE STATEMENT

1.01 Information Technology ("IT") is widespread and critical to Cameron County operations. IT is essential in managing the transactions, information, and knowledge necessary to initiate and sustain the county. Usage of IT resources needs to be appropriately governed and managed to ensure that it brings value to Cameron County ("CC") and that potential risks and security threats are adequately mitigated or addressed. The purpose of this "End User Computing Policy" ("EUCP") is to expound on your responsibilities as a user of Cameron County's computing resources, the relevant County policies in relation to the authorized and lawful use of CC's computing resources, and the appropriate and consistent levels of security controls to be maintained across computing environments. In view of the evolving nature of Information technology and the laws and regulations governing information technology, The Information Systems department and Cameron County Legal may review and modify this policy whenever deemed appropriate.

1.02 This policy applies to all Cameron County employees (permanent and temporary) and non-employees (e.g. contractors, consultants,) who are authorized to use CC's computing resources ("Users"). In this Policy, "Cameron County's computing resources" refers to all computing equipment, devices and information systems that are owned or leased by Cameron County, including but are not limited to personal computers (i.e. PCs or desktops), notebooks (i.e. laptops), tablets, smartphones (i.e. advanced mobile telephonic devices with e-mailing capabilities) and other computer equipment, voice networks, software, servers, operating systems and storage media.

II. AUTHORITY

2.1 The responsibility and authority to govern the use of county computers and network resources are assigned by the Commissioners' Court to the Cameron County Information Technology Systems Department and as it pertains to the Department Director, Appointed or Elected Official.

III. DEFINITIONS

3.1 Cameron County – a local governing body known as the Commissioners' Court.

3.2 Computer Network Resources – includes computers, computer equipment, computer assistance services, software, computer accounts provided by Cameron County, information resources, electronic communication facilities (including electronic mail, telephone mail, Internet access, network access), or systems with similar functions.

3.3 Confidential information - information maintained by Cameron County that is exempt from disclosure under the provisions of the Texas Open Records Act or other state or federal law, attorney work product, attorney-client privileged, and law enforcement communications.

3.4 Information resources – data or information, software, and hardware that render data or information available to users.

3.5 Misuse - any activity of a user or other person who engages in the inappropriate use of computing resources.

3.6 Network – a group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.

3.7 Peripherals – special purpose devices attached to a computer or computer network, such as printers, scanners, plotters, and similar equipment.

3.8 Sensitive information – Sensitive information is data that must be protected from unauthorized access to safeguard the privacy or security of an individual or organization. This can include Personal information, Business information, and classified information.

3.9 Server – a computer that contains information shared by another computer on a network.

3.10 Software – programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, etc.) usually referred to as computer programs.

3.11 Network System Administrator – administrator to include the Chief Technology Officer or authorized staff employed by the Cameron County Information Technology Systems whose responsibilities include a system, site, or network administration. Network System Administrators perform functions including, but not limited to, installing hardware, software, managing a computer or network, and keeping a computer system in operation.

3.12 User – any individual who uses, logs in, attempts to use, or attempts to log in to a system, whether by direct connection or across one or more networks or who attempts to connect to or traverse a network, whether via hardware, software or both. Each user is responsible for his or her use of the computer resources and for learning proper data management strategies.

3.13 Social Media - websites and applications that enable users to create and share content or to participate in social networking. The U.S. Government defines social media as the various activities that integrate technology, social interaction and content creation.

IV. User Roles and Responsibilities

4.1 Users must subscribe to the highest degree of ethical behavior while using Cameron County's computing resources. Any attempt to hide, forge or otherwise represent another identity (e.g. steal another person's password) is prohibited.

4.2 Users must take personal responsibility for the security of individually assigned computing equipment and the business information residing in the systems. Users must not make any hardware modifications to CC's computing resources without appropriate written approval from the Information Systems Department.

4.3 Users should ensure the physical security of mobile computer equipment (e.g. smartphones, tablet, and notebooks) assigned to them. Any loss of mobile computer equipment must be reported to both Department Head and Chief Technology Officer for immediate investigation. In the case of loss due to negligence, Users may be required to compensate Cameron County for the lost asset.

4.4 Users must ensure that only authorized software is used. The authorized software is software that strictly complies with the following:

4.4.1 Licensed for business use. This includes the right of use associated with Freeware, Shareware and Open Source Software; and

4.4.2 Approved by Information Systems Department for use. If Users are in any doubt as to the license status of their software, they should contact the Information Systems department to verify the status of the software license.

4.4.3 Authorized software installed in Cameron County computing systems must not be removed without prior written approval by their respective Department Head and Information Systems.

4.4.4 Malicious software (e.g. hacking software, port scanning, password sniffer etc.) shall not be installed in any computing systems connected to Cameron County network.

4.5 Users are encouraged to conduct regular backups and store important data on network servers. If the user chooses to backup to external backup media (Flash Drive, Portable Hard Drive…) and includes confidential information, the device must be stored in a secure environment.

4.6 Personal computing equipment such as personal computers (PCs) and laptops should not be configured to provide peer-to-peer file sharing or web application services (such as Skype, Spotify, BitTorrent, etc.) unless appropriate written authorization from the respective department head and Information Systems has been obtained.

4.7 Computing equipment that has been installed at an assigned location should not be moved unless appropriate written authorization from Department Head and Chief Technology Officer has been obtained to move such equipment. For shared computing equipment, appropriate security measures must be in place to prevent unauthorized access to confidential information (e.g. password protection of confidential documents).

4.8 All access to information shall be on a "need to know basis".

4.9 Users shall not engage or attempt to engage in any of the following activities:

4.9.1 Access systems that he/she is not authorized to access;

4.9.2 Masquerade as another account holder;

4.9.3 Circumvent security systems;

4.9.4 Exploit or probe for security vulnerabilities on Cameron County's IT systems and network or other organizations' networks;

4.10 Deliberately damaging or attacking or degrading of the performance of Cameron County's IT systems and network or that of any other organization.

4.11 Users should contact Chief Technology Officer should there be any doubt as to the applicable laws, agreements or other requirements.

4.12 Users, whether accessing Cameron County's computing resources from within the premises or outside via VPN or other such remote access, such as in homes, hotels, cyber-cafes or the premises of customers or business associates, are subject to the same rules and regulations as set out in this End User Computing Policy.

4.13 Only Cameron County supplied PCs, notebooks, and tablets shall be connected to the Cameron County network;

4.14 All PCs and notebooks connected to the Cameron County network shall be installed and updated promptly with anti-virus software approved by the county and updated promptly with relevant security patches.

4.15 Any 3rd party PCs, notebooks, and tablets connected to the Cameron County Network remotely via any means including but not limited to VPN must be approved by the Commissioner's Court and renewable every three (3) years.

4.16 Users do not have the right to allow/permit any 3rd party or non-county entity to remotely access their assigned desktop or any networked county resource.

V. PHYSICAL AND ENVIRONMENTAL SECURITY

5.1 Users of personal computing equipment must configure their password-protected screen-savers to activate after 15 minutes of inactivity to prevent unauthorized access to county data when they are away from their computers.

5.2 Laptops and other mobile computing devices should be physically secured when left unattended in an unsecured environment (e.g. hotel function rooms) for any period of time.

5.3 Users should log off and shut down their desktop systems before they leave their office, unless otherwise specifically authorized or instructed in writing by their respective Department Head or Information Systems. Laptops should be kept in a locked drawer or room after office hours.

5.4 Heads of Departments/Supervisors are encouraged to conduct regular checks or audits to ensure that Cameron County's computing resources are constantly secured and not left unattended.

VI. PASSWORD MANAGEMENT

6.1 Users must ensure that user identities (IDs) and passwords assigned to them are kept confidential and are not shared with others, including colleagues, team members or managers.

6.2 User IDs and passwords must be memorized and not written down, electronically stored (unless they are appropriately encrypted), or be posted anywhere.

6.3 Default password must be changed upon the first login. Users are expected to change their passwords regularly depending on the confidentiality of the information. As a guide, passwords should be changed every 90 days.

6.4 Users must use strong passwords for all CC's computing resources. Strong passwords should have at least 8 alphanumeric characters including letters and numbers. Users must not use weak passwords as this may compromise access to CC's computing resources. Examples of weak passwords are:

6.4.1 Names of relatives, friends or colleagues
6.4.2 Birth dates
6.4.3 Telephone numbers
6.4.4 User Login ID
6.4.5 Repeated characters or numbers, e.g. 66666666
6.4.6 Words that can be found in dictionaries

6.5 Users should not re-use passwords that have been used within the last three changes.

6.6 Users should use unique passwords to access different systems.

6.7 If Users suspect that their passwords have been compromised, they should change their password and inform Information Systems immediately.

6.8 Users must not share passwords with anyone, this includes but is not limited to other county employees, vendors, or other non-county entities.

6.9 When a password reset is required, the user will need to have their supervisor submit a formal request (Email or helpdesk ticket) to verify the identity of the person.

VII. E-MAIL

Cameron County e-mail system is designed to improve service to our employees, enhance internal communications, and reduce paperwork. Employees using Cameron County e-mail system must adhere to the following policies and procedures:

7.1 Cameron County e-mail system, network, and Internet/Intranet access are intended for business-use only. Employees may access e-mail and the Internet for personal use only during non-working hours, and strictly in compliance with the terms of this policy.

7.2 All information created, sent, or received via Cameron County e-mail system, network, Internet, or Intranet, including all e-mail messages and electronic files, is the property of Cameron County. Employees shall have no expectation of privacy regarding this information. Cameron County reserves the rights to access, read, review, monitor, and copy all messages and files on its computer systems at any time and without notice.

7.3 Users should be careful when expressing facts, opinion, intention etc. via e-mail as such statements may legally bind the Users and/or Cameron County and can be produced in Court or other dispute resolution forums in the same way as oral or written statements. E-mails should be used sensibly and professionally to avoid negative publicity, exposing CC and/or the Users to legal liabilities.

7.4 When deemed necessary, Cameron County reserves the right to disclose text or images to law enforcement agencies or other third parties without the employee's consent. Extreme caution shall be used by the employee to ensure that the correct e-mail address is used for the intended recipient(s).

7.4.1 Users should ensure that e-mails, especially those containing confidential information, are sent to the correct addresses. Users are advised to double-check the address list before sending an email.

7.4.2 When Users receive an e-mail that has been sent in error, it is the User's duty to immediately contact the sender by return e-mail and then irretrievably delete the email from their system.

7.5 Confidential information should not be sent via e-mail unless clearly identified in the email as confidential by including in the e-mail the word "CONFIDENTIAL" prominently displayed, or unless encrypted by Cameron County approved encryption software and according to established Cameron County procedure in use at the time of transmittal. This includes the transmission of vendor financial information, Social Security numbers, employee health records, attorney-client communications or other confidential material.

7.6 Users must not use public file hosting or could storage services (e.g. Dropbox, SkyDrive, Google Drive etc.) to backup, store, send or distribute company information. Unless authorized by the Commissioner's Court

7.7 Only Elected Officials, Appointed Department Heads, or authorized Supervisors (authorized by their Elected or Appointed Department Head) within their own department shall be permitted to access another person's e-mail without consent. No supervisor Appointed Department Head or Elected Official shall access or have the Computer Center Access an employee's email, if such employee is not in their department, without prior approval of the Commissioners Court. (This provision does not apply to a Court Order addressed to and served on the County Judge in the same manner as a citation is served under V.T.C.A., C.P.R.C., Section 17.024(a).)

7.8 No Supervisor, Appointed Department Head or Elected Official shall access another Supervisor's, Appointed Department Head's or Elected Official's e-mail without prior approval of the Commissioners Court. (This provision does not apply to a Court Order addressed to and served on the County Judge in the same manner as a citation is served under V.T.C.A., C.P.R.C., Section 17.024(a).)

7.9 E-mail messages shall contain professional and appropriate language at all times. Employees are prohibited from sending abusive, harassing, intimidating, threatening, and discriminatory or otherwise offensive messages via email

7.10 All messages archived in Cameron County computer systems shall be deemed County property, as is all information on Cameron County systems. Employees shall have the responsibility for verifying and understanding Cameron County email policies as prescribed by their applicable department. Employees shall save or print important messages to prevent them from being accidentally deleted.

7.11 Misuse and/or abuse of electronic access, including but not limited to, personal use during working hours, copying or downloading copyrighted materials, visiting pornographic sites or sending abusive e-mail messages shall result in disciplinary action, up to and including termination.

7.12 Please be aware the Cameron County E-Mail is for the sole purpose of Cameron county work and not to be used for any personal activities or for registering for personal sites and services.

7.13 Sensitive or confidential emails relating to law enforcement communications shall not be accessed without authorization for release by the District Attorney. Open Information requests for law enforcement information shall be immediate, upon receipt, forwarded to the District Attorney's Office for its review in accordance with Chapter 552 Prosecutorial Exception, Section 552.108.

7.14 E-mails or other information relating to attorney work product and attorney-client "confidential" or "privileged" information shall be protected and shall not be accessed except in strict compliance with Texas State Bar Rules, including but not limited to Rules 1.05 and 1.12.

7.15 E-mail contents may be considered public records and subject to disclosure under Texas Public Information Act. A public information request for the production of e-mail on a County e-mail box shall be referred to County Counsel for review and response.

7.16 County E-mail added to any mobile device whether County or personally owned may be subject to a public information request.

7.17 Should a mobile device with County Email be lost or stolen, you are required to contact the IT Department to remotely wipe off the e-mail or complete phone for security purposes. A person who has separated from the County must also remove County email from their mobile devices, the IT department reserves the right to remotely remove upon notification of separation.

VIII. NETWORK AND INTERNET/INTRANET

8.1 PERSONAL RESPONSIBILITY

By accepting an account, password, related information, or the accessing Cameron County Network, an employee shall agree to adhere to this End User Compliance Policy regarding their use and agree to report any misuse or policy violation(s) to their supervisor and the Cameron County Chief Technology Officer.

8.1.1 Use of Network Resources and the Internet is a privilege, not a right. Use of Network and Internet access extends throughout an employee's term of employment, providing the employee does not violate Cameron County policies regarding Network, Internet or Intranet use. Department Heads shall be responsible for the identification of both appropriate and inappropriate use.

8.1.2 Cameron County reserves the right to suspend access at any time, without notice, for technical reasons, possible policy violation, security or other concerns.

8.1.3 Network Resources and Internet access is provided as a tool for our organization's business. Cameron County reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all usage of the Network and the Internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of Cameron County. An employee should have NO expectation of privacy.

Initials: _____

8.1.4 Employees shall not download application files from the Internet without the prior authorization of direct management. Any files authorized for download from the Internet must be scanned with virus detection software before being opened.

8.1.5 Cameron County reserves the right to block or prevent access to any internet content it deems offensive or unsuitable for the work environment without any prior notification.

8.2 CONFIDENTIAL INFORMATION

8.2.1 Certain employees may have access to confidential information regarding Cameron County, other employees, and clients. With the approval of management, employees shall use e-mail to communicate confidential information internally as requested. Such e-mail must be marked "Confidential." For purposes of this policy, confidential information includes, but is not limited to:

8.2.1.1 all trade secrets, know-how, business and financial information and other proprietary information or data disclosed to one party by the other or incorporated in materials or products provided to one party by the other and marked or indicated to be confidential

8.2.1.2 Employee Information, such as social security number, address, date of birth, marital status.

8.2.1.3 Health & Medical Information, any health and medical information about employees must also be kept confidential under the following laws (in addition to any applicable state laws):

a. Americans with Disabilities Act (ADA)
b. Health Insurance Portability and Accountability Act (HIPAA)
c. Genetic Information Nondiscrimination Act (GINA)
d. Family and Medical Leave Act (FMLA)
e. Workers' Compensation

8.2.2 Criminal or Justice related Information, any criminal or legal information about pending cases must also be kept confidential under the following laws (in addition to any applicable state laws):

a. Criminal Justice Information Services Division (CJIS)

8.2.3 Procedures for computer access and passwords of Cameron County users, program annuals, user manuals, or other documentation, run books, screen, file, or database layouts, systems flowcharts, and all documentation normally related to the design or implementation of any computer programs

developed by Cameron County relating to computer programs or systems installed for the users;

8.2.4 Lists of present clients, customers, and vendors and the names of individuals at each client or customer location with whom Cameron County deals, the type of equipment or computer software they purchase or use, and the information relating to those clients, customers, and vendors which has been given to Cameron County by them or developed by Cameron County, relating to computer programs an or systems installed;

8.2.5 Lists of or information about personnel seeking employment with or who are currently employed by Cameron County;

8.2.6 Any other information relating to Cameron County engineering, marketing, merchandising, and purchasing or selling of land.

8.2.7 Any information relating to attorney work product, attorney-client privilege, and law enforcement communications.

8.3 PROHIBITED ACTIVITIES

8.3.1 Employees shall be prohibited from using Cameron County e-mail system, network, or Internet/Intranet access for the following activities:

8.3.1.1 Downloading software without the prior written approval of Cameron County Chief Technology Officer or the direct supervisor's approval.

8.3.1.2 Printing or distributing copyrighted materials. This includes but is not limited to, software, articles, and graphics protected by copyright laws.

8.3.1.3 Using software that is not licensed by the manufacturer or approved by the Cameron County Chief Technology Officer.

8.3.1.4 Sending, printing, or otherwise disseminating Cameron County propriety data or any other information deemed confidential by Cameron County, to unauthorized persons.

8.3.1.5 Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment.

8.3.1.6 Making offensive or harassing statements based on race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.

8.3.1.7 Sending or forwarding messages containing defamatory, obscene, offensive, or harassing statements. An employee should notify their supervisor and/or Human Resource Manager immediately upon receiving such a message. This type of message should not be forwarded.

8.3.1.8 Sending or forwarding a message that discloses personal information without Cameron County authorization. This shall also include accessing, transmitting, receiving, or seeking confidential information about clients or fellow employees with authorization.

8.3.1.9 Sending ethnic, sexual-preference or gender-related slurs and/or jokes via e-mail. "Jokes", which often contain objectionable material, are easily misconstrued when communicated electronically.

8.3.1.10 Sending or soliciting sexually oriented messages or images.

8.3.1.11 Attempting to access or visit sites featuring pornography, terrorism, espionage, theft, or drugs.

8.3.1.12 Gambling or engaging in any other criminal activity in violation of local, state, or federal law.

8.3.2 Participating in activities, including the preparation or dissemination of content, which could damage Cameron County professional image, reputation and/or financial stability.

8.3.3 Permitting or granting use of an e-mail or system account to another employee or persons outside Cameron County. Permitting another person to use an account or password to access the Network or the Internet, including, but is not limited to, someone whose access has been denied or terminated, is a violation of this policy.

8.3.4 Using another employee's password or impersonating another person while communicating or accessing the Network or Internet.

8.3.5 Intentionally introducing a virus, harmful component, corrupted data or the malicious tampering with any of Cameron County computer systems.

8.4 COMPUTER VIRUS / MALWARE

8.4.1 Users who are non-Cameron County employees must ensure that their own or company's personal computing equipment is installed with authorized anti-virus software at all times when utilizing CC's computing resources (e.g. connecting to CC's network system). Users who are Cameron County employees must ensure that their personal computing equipment is in their possession at all times and have an authorized anti-virus software installed.

8.4.2 Users should check that the anti-virus software is activated and virus signatures are up-to-date on such personal computing equipment. Users are not to de-activate the anti-virus software, even temporarily, without the written approval of the Information Systems department

8.4.3 Users should scan their drives, folders, and files regularly for viruses and any other unauthorized software.

8.4.4 Visiting Internet sites, downloading or opening of files or attachments (especially unfamiliar ones) may introduce viruses into CC's computing systems. Any file downloaded from the Internet should be scanned by anti-virus software before it is opened or run.

8.4.5 Users must not download, develop or execute viruses, spyware and spamming tools.

8.4.6 Users are strongly discouraged from opening any emails or access web contents from unfamiliar senders or web pages. If in doubt over the nature of a file or attachment, please consult your system administrator.

8.5 MONITORING AND COMPLIANCE

8.5.1 As Cameron County's computing resources are granted to users for business purposes only, Cameron County Management reserves the right to monitor the use and contents of electronic and voice mail communications (e.g., email, telephone voice recording) and the information/data stored (e.g., business transactions, audit logs) on Cameron County's computing resources (e.g., PCs, laptops, servers) at any time without notice to Users. Such monitoring shall be led by the Chief Technology Officer and shall only be carried out on the Commissioners Court's written authorization and approval.

8.5.2 Non-compliance with this policy may result in disciplinary action including termination of employment and, in the case of users who are not Cameron County employees, the termination of the business contract or consulting services. Criminal and/or civil action may also be pursued if Cameron County deems it fit. Any person who aids or abets the violation of this policy shall also face the same consequences.

8.5.3 Any failure to impose disciplinary action on any person for any non-compliance at any point in time shall not be deemed to be a waiver of the right of Cameron County to take any disciplinary actions whatsoever. In the case of Users who are not Cameron County employees, any failure to take any action for any non-compliance at any point in time shall not be deemed to be a waiver of the rights of Cameron County as against such Users.

8.5.4 Users are required to read this policy carefully for compliance. They are required to agree to comply with this policy when they apply for new user accounts.

IX. SOCIAL MEDIA

9.1 Social media is any tool or service that facilitates conversations over the Internet. Social media may include but is not limited to:

9.1.1 Social network sites (e.g. Facebook, Google+, LinkedIn)

9.1.2 Blogging and micro-blogging sites (e.g. personal blogs, Twitter)

9.1.3 Wikis (e.g. Wikipedia)

9.1.4 Online forums and discussion boards

9.1.5 Video and photo sharing websites (e.g. YouTube, Flickr, Instagram)

9.1.6 Instant messaging services (e.g. SMS, WhatsApp, Skype)

9.2 Users must not represent Cameron County on any social media platform unless expressly authorized by the County Commissioner's Court. The creation and management of County account on social media is the sole prerogative and responsibility of Cameron County Management (Commissioner's Court).

9.2.1 Requirements for Department's Using Social Media

9.2.1.1 Establish a well thought out social media work plan that complements countywide policies and considers the department's mission and goals, audience, legal risks, technical capabilities, security issues, emergency response procedures, etc. The work plan shall be submitted to IT and County Administrator's Office for review.

9.2.1.2 Designate a Social Media Coordinator responsible for overseeing the department's social media activity, policy compliance, and security protection.

9.2.1.3 Designated Social Media Coordinator should be vetted by IT to ensure required skill set is evident and the person has adequate experience with various Social Media tools.

9.2.1.4 County social media network accounts shall be created using an official County email account.

9.2.1.5 Contact information should display an official County email address, include something about being the "official account", and provide a link to the County or department website.

9.2.1.6 The name "Cameron County" or the official County or department logo must be displayed.

9.2.2 Requesting and obtaining Authorized Use

9.2.2.1 Department Heads, or designees, are responsible for designating appropriate levels of use.

9.2.2.2 Social media network usage shall be limited only to those with a clear business purpose to use the forum.

9.2.2.3 Appropriate usage levels include identifying what sites the individual is approved to use, as well as defining capability: publish, edit, comment or view only.

9.2.2.4 Social Media Coordinators shall review site activity daily for exploitation or misuse.

9.3 Users must not disclose or discuss any matters concerning Cameron County business over social media unless authorized by the Commissioner's Court.

9.3.1 Only official spokespersons, Public Information Officers, Social Media Coordinators, and Department Head designee shall be considered authorized users and have permission to post and respond.

9.3.2 Authorized users shall review the County's social media policies and procedures and are required to acknowledge their understanding and acceptance of their scope of responsibility <u>via signing an acknowledgment form and forwarding to IT.</u>

9.3.3 Contents posted on County social media sites may be considered public records subject to disclosure under Texas Public Information Act. Public Information Request requests for the production of posts

on a County social media site shall be referred to County Counsel for review and response.

9.4 The user must not disclose any information that is confidential or proprietary to Cameron County or any third-party that has provided such information to Cameron County. Such information includes, without limitation, financial information, personal data, information concerning legal proceedings or matters, internal issues and information in connection with or which could jeopardize Cameron County's operations or intellectual property rights.

9.5 Users should take precaution when posting personal information on social media sites to protect personal privacy and prevent identity theft or other crimes such as stalking.

9.6 Users must exercise sound judgment before posting any comments, opinions or remarks over social media. Users must comply with all applicable laws when using social media.

9.6.1 Authorized users shall do so only within the scope defined by their respective department and in compliance with all County policies, practices and user agreements and guidelines.

9.6.2 Violations of this policy shall be reviewed on a case-by-case basis and may result in appropriate disciplinary actions.

9.7 Users must not post remarks that are obscene, derogatory, insensitive, racially and culturally offensive or use social media in any way to attack or abuse another person.

9.8 Users must not post any copyrighted information (music, videos, text, etc.) belonging to third parties without permission from the owner.

9.9 Users must neither claim nor imply that they are speaking on behalf of Cameron County unless authorized in writing by the Commissioner's Court. As and when necessary, Users should add the disclaimer *"The opinions and positions expressed are my own and not those of Cameron County or the Commissioner's Court"*.

9.10 Users must be mindful of the information that they disclose on social media and should act in a manner which does not bring Cameron County's image and reputation into disrepute.

9.10.1 Profane language or content;

9.10.2 Content that promotes fosters or perpetuates the discrimination of protected classes;

9.10.3 Sexual harassment content;

9.10.4 Solicitations of commerce or advertisements including promotion or endorsement;

9.10.5 Promotion or endorsement of political issues, groups or individuals;

9.10.6 Conduct or encouragement of illegal activity;

9.10.7 Information that may tend to compromise the safety or security of the public or public systems;

9.10.8 Content intended to defame any person, group or organization;

9.10.9 Content that violates a legal ownership interest of any other party, such as trademark or copyright infringement;

9.10.10 Making or publishing of false, vicious or malicious statements concerning any employee, the County or its operations;

9.10.11 Violent or threatening content;

9.10.12 Disclosure of confidential, sensitive or proprietary information;

9.11 Users are personally responsible for the content that they post on social media and should only post on behalf of Cameron County where expressly authorized in writing by the Commissioner's Court.

9.12 Departments shall only utilize County approved social media networks for hosting official County social media sites.

9.12.1 New social media networks under consideration will be reviewed and approved by the County Administrator's Office and ITS Chief Information Officer with consultation from County Counsel and Human Resources when appropriate.

9.12.2 Departments may request review and approval of additional social media networks to IT as needed.

X. COMPUTER SOFTWARE USAGE, MAINTENANCE, AND EQUIPMENT

10.1 Employees shall use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software (except during the daily backup routine) is a violation of copyright law.

10.2 To ensure compliance with software license agreements and Cameron County Software Usage Policy, the employee shall adhere to the following:

10.2.1 Cameron County software shall not be removed from the premises or copied for personal use. No software shall be brought into Cameron County and installed on Cameron County computers without a written permission of the Chief Technology Officer.

10.2.1.1 When such permission is obtained, the software will be installed by the Computer Center Operations Staff in accordance with licensing agreements only.

10.2.1.2 Cameron County Computers and supporting hardware are purchased through the Cameron County Computer Center and are done so with certain criteria and standards, See Cameron County Equipment Standards Policy.

10.2.2 Cameron County prohibits the unauthorized duplication of software. Employees illegally reproducing software shall be subject to disciplinary action up to and including termination. In addition, employees illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment

10.2.3 Requests for new software beneficial to the mission of Cameron County shall be made through the Computer Center or Department Head.

10.2.4 Third party/personal software shall not be installed on the desktop, thin client, laptop or network computers without permission of the Chief Technology Officer (i.e. screensaver, P2P programs, or music/video streaming software including but not limited to shareware or freeware.) Software loaded on individual computers is subject to review at any time, and unauthorized software will be removed.

10.2.5 If an employee is required to work or use the software at home, Cameron County shall purchase an additional copy or license if deemed necessary by the Chief Technology Officer or Department Head. Any employee that is issued such software shall use the software accordingly and understand that the software is the property of Cameron County and will only be used in good order and discipline and not for non-work-related items.

10.2.6 Any software that has been released by the Chief Technology Officer for home use shall require a custody release form approved by the Department Head prior to removal from the Cameron County confines.

10.2.7 Unauthorized personnel should not be allowed to access or use Cameron County computers either in the Cameron County office space or in the homes of employees.

10.2.8 Any employee, who knowingly installs, makes, acquires, or uses unauthorized copies of software not licensed to Cameron County shall be subject to disciplinary action, up to and including termination.

10.2.9 Anti-virus software shall be installed and configured on all Cameron County computers by the Cameron County Operations Staff, and shall not be shut down for any reason.

10.2.10 Media sharing software of any kind is not permitted on Cameron County Computers; this includes but is not limited to any form of P2P/BitTorrent or any of its current incarnations.

10.3 Maintenance of Cameron County Computer Equipment shall be done by the IT Department Operations Staff or approved outside entity. If an operating system or upgrade is necessary, please contact the IT Department Staff prior to any instance, this includes but is not limited to Internet Browsers, Operating System Upgrades or updates, media players, drivers or any other software not previously mentioned. For any major or emergency maintenance, proper notice will be sent out to staff with the intended schedule, completion time, and impacted systems.

10.4 Computer Network Hubs, switches, routers, or print servers shall not be added to the network, all additional hardware will be approved by the Chief Technology Officer prior to the procurement of any additional hardware.

10.5 Personal computer items such as Apple iPad, Android Tablets, or Smart Phones or any such entity shall not be connected to Cameron County Network Computers unless specifically purchased through Cameron County. These items are subject to information theft just like laptop computers and require extra diligence in safeguarding them when they are connected and removed from the confines of Cameron County.

10.5.1 These devices are allowed to connect to Cameron County provided public Wi-Fi.

10.6 Computers (i.e. Desktop, Thin-Client, Servers, Tablets or Laptops) as a whole are considered one entity, the replacement, addition, or removal of any internal/external component to any such entity is strongly prohibited. If more memory, hard disk, or repair to any item is needed, contact the Computer Center Helpdesk Staff.

10.7 Telecommunications equipment and services shall be procured and configured through the IT Department Operations Staff. Contact the IT Department Operations Staff if repair, Maintenance, or relocation of telecommunication services are required, this includes but is not limited to IPFlex, PBX, MPLS type circuits, Internet or other items not listed.

XI. ENFORCEMENT - COMPLIANCE AND NONCOMPLIANCE

11.1 Management personnel shall be responsible for ensuring employee compliance with Cameron County Policy and shall immediately report the violation to their direct supervisor, Department Head, Cameron County Chief Technology Officer and/or the Administrative Services Director.

11.2 Violation of these policies shall result in disciplinary action up to and including termination. It is important to note that failure to adhere to this Policy may lead to the cancellation of a user's computer account(s), suspension, dismissal, or other disciplinary action by Cameron County as well as referral to legal and law enforcement agencies.

11.3 All infractions will be subject to but not limited to Cameron County's existing Disciplinary Policy.

REFERENCES

1. **The following is a list of some laws that pertain to computer usage, the list is not encompassing:**

   a. Texas Administrative Code, 202: Information Security Standards
   b. Texas Penal Code, Chapter 33: Computer Crimes
   c. Texas Penal Code, Chapter 33.07: Online Harassment
   d. Texas Penal Code, Chapter 37: Tampering with Government Record
   e. The United States Penal Code, Title 18, Chapter 47 Fraud and False Statements, Section 1030: Fraud and related activity in connection with computers.
   a. Computer Fraud and Abuse Act of 1986 (Title 18 U.S.C Section 1030)
   b. Computer Abuse Amendments Act of 1994
   c. Federal Copyright Law
   d. Digital Millennium Copyright Act of 1998
   e. Electronic Communication Privacy Act 1986
   f. Computer Software Rental Amendments Act 1990
   g. Homeland Security Act H.R. 5005 November 2002
   h. Title 18, United States Code, Section 2701: Unlawful Access to Stored Communications
   i. Title 18, United States Code, Section 1037: CAN-SPAM Act

2. **Referenced Legal Documents**

   a. CIVIL PRACTICE AND REMEDIES CODE - Sec. 17.024. SERVICE ON POLITICAL SUBDIVISION.
      (a) In a suit against a county, the citation must be served on the county judge.
      (b) In a suit against an incorporated city, town, or village, a citation may be served on the mayor, clerk, secretary, or treasurer.
      (c) In a suit against a school district, a citation may be served on the president of the school board or on the superintendent.
      Acts 1985, 69th Leg., ch. 959, Sec. 1, eff. Sept. 1, 1985.
   b. GOVERNMENT CODE - TITLE 5. OPEN GOVERNMENT; ETHICS
      Sec. 552.108. EXCEPTION: CERTAIN LAW ENFORCEMENT, CORRECTIONS, AND PROSECUTORIAL INFORMATION.
      (a) Information held by a law enforcement agency or prosecutor that deals with the detection, investigation, or prosecution of crime are accepted from the requirements of Section 552.021 if:
      (1) The release of the information would interfere with the detection, investigation, or prosecution of crime;
      (2) It is information that deals with the detection, investigation, or prosecution of crime only in relation to an investigation that did not result in conviction or deferred adjudication;
      (3) it is information relating to a threat against a peace officer or detention officer collected or disseminated under Section 411.048; or
      (4) It is information that:

      Added by Acts 1993, 73rd Leg., ch. 268, Sec. 1, eff. Sept. 1, 1993. Amended by Acts 1995, 74th Leg., ch. 1035, Sec. 7, eff. Sept. 1, 1995; Acts 1997, 75th Leg., ch. 1231, Sec. 1, eff. Sept. 1, 1997; Acts 2001, 77th Leg., ch. 474, Sec. 6, eff. Sept. 1, 2001.
      Amended by:
      Acts 2005, 79th Leg., Ch. 557 (H.B. 1262), Sec. 3, eff. September 1, 2005.
      Acts 2005, 79th Leg., Ch. 557 (H.B. 1262), Sec. 4, eff. September 1, 2005.

   c. Texas State Bar Rules

      i. Rule 1.05. Confidentiality of Information

         "Confidential information" includes both "privileged information" and "unprivileged client information." "Privileged information" refers to the information of a client protected by the lawyer-client privilege of Rule 503 of the Texas Rules of Evidence or of Rule 503 of the Texas Rules of Criminal Evidence or by the principles of attorney-client privilege governed by Rule 501 of the Federal Rules of Evidence for United States Courts and Magistrates. "Unprivileged client information" means all information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client.

ii. Rule 1.12. Organization as a Client

(a) A lawyer employed or retained by an organization represents the entity. While the lawyer in the ordinary course of working relationships may report to, and accept direction from, an entity's duly authorized constituents, in the situations described in paragraph (b) the lawyer shall proceed as reasonably necessary in the best interest of the organization without involving unreasonable risks of disrupting the organization and of revealing information relating to the representation to persons outside the organization.

IX. APPENDICES

Appendix A: Cameron County Computer User Access Agreement & Policy Guidelines

Cameron County End User Compliance Policy and Purpose Statement

This policy governs the use of technology equipment and related devices operated by Cameron County employees for connection County related applications and internet-based services. The purpose of these guidelines is to help maximize the effective use of these County resources. The intent of these policy guidelines is to permit maximum freedom of use consistent with Federal and State Law, Cameron County policy, and a productive working environment.

The following is a list of policy guidelines that shall be followed by Cameron County employees who have access and use of computer equipment and software. These guidelines highlight the policies and procedures sections I-IX as to the use, safety, and maintenance of your computer and equipment.

1. A user shall only utilize the network and computer resources solely for the purpose of their job requirements or needs.
2. A user shall not install any third-party software on their desktop computers or network computers without the permission of the Chief Technology Officer or Computer Center Staff.
3. A user shall not utilize the Internet Connection in a means not conducive to the normal daily routine, including inappropriate websites with adult themes, slanderous themes, hate sites, or pornographic sites that may be deemed offensive or inappropriate for the workplace.
4. A user shall not download or install any Internet Radio services or utilize any form of peer-to-peer applications to obtain any illegal or unlicensed media or software.
5. A user shall not provide any Internet Sharing Resource for personal gain to outside entities not physically located within the Cameron County Organization.
6. A user shall not utilize the email services provided to support Spam sessions, or to spread non-work-related information that could potentially cause the spread of virus, worm or other malicious code.
7. A user shall not install or introduce to the network any computer, laptop, workstation, or computer peripheral other than those provided by the Cameron Computer Center.
8. A user shall report any and all unauthorized use of the Cameron County Information Systems Network to the Computer Center Staff immediately to maintain network integrity.
9. The user shall not have any expectations of privacy when it comes to accessing the County's technology infrastructure, services, or provided internet access.
10. A user shall not share their password with another user unless strictly allowed by their Department Head, and solely for the purpose of completing a task necessary to the workplace or for the good of Cameron County.
11. Any user who suspects that their computer or workstation may be infected by any malicious code (i.e. virus) shall report the incident promptly to the Computer Center Staff for investigation and removal.
12. A user shall log out and power down their workstation at the end of every workday and before any weekend or extended Holiday period to maintain security and integrity of the network unless otherwise noted.
13. A user shall not attempt to fix or reinstall components or Operating Systems onto their workstation by any means without the consent of Computer Center Staff; this includes new versions of media players, Internet browsers, drivers or general updates.
14. A user shall not use applications like P2P/Bit torrent clients on their workstation; which can share personal information with the Internet.
15. A user shall try to keep backup copies of important email and documents, in case of a hard drive failure; this will help retain important information that may not be accessible in a timely manner.

16. All users shall make their passwords 6 - 8 characters long, using numbers, letters, uppercase/lowercase, and special characters together to make passwords more secure, a good example = (Kool-Aid ~ K00la1D).

15. When traveling by air, always carry the laptop on the airplane. Never check the laptop as baggage and never put the laptop inside another case checked as baggage. The only exception to this is that a laptop can be shipped in a special shipping container with padded foam for shipping sensitive items. That case is specially constructed and designed to house sensitive electronic equipment.

16. Always hand-carry the laptop when traveling to and from the airport. Don't put it in the trunk of a cab or on the rack of an airport shuttle.

17. If you have the need to carry a desktop computer home to work on Cameron County projects, the computer must be carried to and from the office on a daily basis during the work week. Under no circumstances will Cameron County property be left at your residence while you are at work.

18. Laptop computers are assigned individually and will not be transferred custody to another user without the notifying the Cameron County Computer Center or the Chief Technology Officer.

19. Plants or other water-based items should not be placed near any part of the assigned computer hardware to prevent the risk of electric shock.

20. The e-mail system is the property of Cameron County and is intended for the furtherance of official business for this County. Messages transmitted or received by the e-mail system are messages and property of Cameron County and are subject to the retention policy.

21. All messages sent on the e-mail system are considered County Property and not personal or confidential messages of the employee.

22. Passwords shall be used to gain access to the e-mail system for the purpose of protecting the integrity of the Cameron County Network and shall be changed frequently to avoid unauthorized access.

23. E-Mail messages are the intellectual property of Cameron County, not of the employees, and must pertain only to Cameron County business.

24. E-Mail messages should not be left on the computer screen when the employee is away from his/her desk or workstation, in order to protect Cameron County proprietary information no information protected by copyright laws, including software, will be sent or copied via e-mail.

25. All messages on the e-mail system are to be businesslike. There will be no tolerance for using the system for personal messages or for those, which contain profanity, vulgarity, and/or harassing or defamatory language.

26. All personnel who use the Cameron County Internet service shall use the service for official business only.

27. If you are unsure of something on your computer screen (email link, pop-up, program), always ask before you click. This is the safest way to avoid infecting your computer equipment or the rest of the network with a virus or leaving Cameron county open to Network attack.

I have read and understood the Cameron County Computer Use – Electronic Access Policies and Procedures and the User Agreement.

Employee Name (Please Print) _____ Department: _____

Employee Signature _____ Date: _____

Information Technology Department

835 E. Levee St. 4th Floor

Brownsville, TX. 78520

(956) 544-0818 or (956) 550-1332

Fax: (956) 550-1337

INFORMATION TECHNOLOGY

helpdesk@co.cameron.tx.us

Information Technology Department

User Management Form

835 E. Levee St. 4th Floor Brownsville, TX. 78521 956-544-0818

Section I: Employee Information (please complete ALL fields)

Name of User: _____ Employee ID: _____

Employee Job Title: _____ E-Mail Address: _____

Supervisor Name: _____

Contact Number: _____

Department Name: _____

Work Address: _____

Requester Signature: _____ Date

Section II: Action Required

☐ New Hire User ☐ Termination ☐ Inter-Department Transfer ☐ Other: _____

Section III: User Services

(*Include Additonal Documentation as Required)

	Add	Remove	Date	Remarks
Instant Messaging (if avail.)	☐	☐		
Email Services	☐	☐		
Internet Access	☐	☐		Standard Access
Odyssey Access	☐	☐		Duplicate Rights of:
Brazos Public Safety	☐	☐		
Mobile Device Email	☐	☐		County Mobile Devices Only, unless otherwise approved
MFA Token (Purchased?)	☐	☐		Tool used to provide additional factor for login
Finance Enterprise Purchasing	☐	☐		Access Requested/Provided by the Auditor's Office
Kronos Access	☐	☐		Access Requested/Provided by the Auditor's Office
	☐	☐		

Section IV: Notes or Special Requirements

Section V: Approval

_____ End User Signature

_____ Department Head Signature

_____ IT Department Representative

*** As per Cameron County End User Compliance Policy signatures are required for this procedure, upon completion of this document an E-Mail Address will be added and/or Internet access granted.

Acceptable uses of company e-mail and Internet access:
The company provides Internet and e-mail access for business usage. Every staff member has the responsibility to maintain and enhance the company's public image and to use company e-mail and access to the Internet in a responsible and productive manner that reflects well on the company. The company recognizes that there will be occasional personal use on lunch breaks and during non-working hours (with the approval of management), but shall not excessive or unreasonable.

Unacceptable uses of company e-mail and Internet access:
The company e-mail and Internet access may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No excessively abusive, profane or offensive language is to be transmitted through the company's e-mail or Internet system. Electronic media may also not be used for any other purpose that is illegal or against company policy or contrary to the company's best interests. Solicitation of non-company business. or any use of the company e-mail or Internet for personal gain, is prohibited. Transmitting of company related data or documentation without management approval is also prohibited.

*** Note to Information Services Department: Please make sure to enter Service call into Help Desk Ticketing System.