CAMERON UNIVERSITY
Computer Use Policy

Policy Statement

Access to modern information technology is essential to the pursuit and achievement of excellence across the Cameron University (CU) mission of instruction, research and academic advancement. The privilege of using computing systems and software, as well as internal and external data networks, is important to all members of the CU community. The preservation of that privilege for the full community requires that each individual student, faculty member, staff member, and administrator comply with institutional and external standards for appropriate use.

Contents

Who Should Know This Policy

President
Vice Presidents
Deans
Department Chairs
Directors
Faculty
Other Accounting/Finance Personnel
Students
Other Groups
All Employees

Responsibilities

Responsible for Policy

University Officer Responsible — Director of Information Technology Services

Procedure

STATEMENT OF PURPOSE: This policy will establish the general guidelines for the use of CU computing resources equipment, services, software, and computer accounts by students, faculty, staff and administration.

1.0 Definitions

1.1 Abuser is any user or other person who engages in misuse of computing resources as defined in Section 2.2 of this Policy.

1.2 Computing resources includes computers, computer equipment, computer assistance services, software, computer accounts provided by CU, information resources, electronic communication facilities (including electronic mail, telephone mail, Internet access, network access), blogs, www browsing, storage media, mobile computing devices or systems with similar functions.

1.3 Computer account is the combination of a user number, username, or userid and a password that allows an individual access to a server or some other shared computer or network.

1.4 Information resources are data or information and the software and hardware that render data or information available to users.

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

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

1.7 Server is a computer or computer program that manages access to a centralized resource or service in a network.

1.8 Software may be programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, etc.). Usually used to refer to computer programs.

1.9 System Administrator is a faculty, staff, or administrator employed by a central computing department such as Information Technology Services whose responsibilities include system, site, or network administration and other faculty, staff or administrators whose duties include system, site, or network administration. System administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. System administrators include any persons responsible for a system which provides the capability to assign accounts to other users.

1.10 User is 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.

2.0 User Responsibility

2.1 Appropriate Use of Computing Resources.

The computing resources provided by CU are primarily intended for teaching, educational, research and administrative purposes, and may generally be used only for authorized CU-related activities. Use of the computing resources is governed by all applicable CU policies, including, but not limited to, sexual harassment, copyright, and student and employee disciplinary policies, as well as by applicable federal, state and local laws. Personally owned computing resources being used to conduct University business are also governed by all applicable CU policies as stated above. (See Institutional Form F11, Faculty and Staff Mobile Email Agreement.)

2.2 Prohibited Use of Computing Resources.

CU characterizes misuse of computing and information resources and privileges as unethical and unacceptable. Misuse constitutes cause for taking disciplinary action. Misuse of computing resources includes, but is not limited to, the following:

a. attempting to modify, remove, or add computer equipment, software, or peripherals without proper authorization;
b. connecting personally owned equipment, such as printers, notebooks, laptops, desktop computers to CU's network; personally owned software may not be installed on CU's computing equipment;
c. accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information or network in question is owned by CU, including but not limited to, abuse, or misuse of networks to which CU belongs or computers at other sites connected to those networks;
d. circumventing or attempting to circumvent normal resource limits, logon procedures and security regulations;
e. sending fraudulent computer mail, breaking into another user's electronic mailbox, or reading another user's electronic mail without his or her permission;
f. sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or vouchers, and fraudulent electronic authorization of purchase requisitions or vouchers;
g. violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization;
h. using CU computing resources to harass or threaten others;
i. using CU computing resources for development, posting, transmission of, or link to, any of the following: commercial or personal advertisements; solutions; promotions; destructive programs; political material; messages which are fraudulent, harassing, obscene, indecent, profane, intimidating, or otherwise unlawful; or any other unauthorized or personal use;
j. taking advantage of another's naivete or negligence to obtain access to any computer account, data, software, or file that does not belong to the user or for which the user has not received explicit authorization to access;
k. physically interfering with other users' access to the CU computing resources;

l. encroaching on others' use of CU computer resources, including but not limited to: disrupting other users' use of computer resources by excessive game playing; by sending electronic chain letters or other excessive messages, either locally or off-campus; printing excessive copies of documents, files, data or programs; modifying system facilities, operating systems, or disk partitions; attempting to crash or tie up a CU or network computer; or damaging or vandalizing CU or network computing resources, equipment, software, or computer files; using Peer-to-peer software; standard computers cannot be used as FTP servers;

m. disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner;

n. data protected by Health Insurance Portability and Accountability Act of 1996 (HIPAA) is prohibited from storage on CU computing resources and being transmitted on CU's network;

o. credit card and banking information is prohibited from storage on CU computing resources and being transmitted on CU's network;

p. reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission;

q. violating any applicable federal, state or local law; or

r. connecting unauthorized servers to any wired network port or to the wireless network.

2.3 User Responsibility.

All users of CU computing resources must act responsibly. Every user is responsible for the integrity of these resources. All users of CU-owned or CU-leased computing resources must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements. It is the policy of CU that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations, and the highest standard of ethics.

2.4 Password Protection.

Each user is responsible for maintaining absolute security of any password or password right granted to the user. Passwords must not be "shared" with another user. Password security helps to protect the CU system against unauthorized access.

2.5 Computing Resource Access.

Access to CU's computing resources is a privilege granted to CU students, faculty, staff and administrators. CU reserves the right to limit, restrict, or extend computing privileges and access to its information resources.

2.6 Freedom of Communication.

It is the intention of CU to maximize freedom of communication for purposes that further the goals of CU. CU places high value on open communication of ideas, including those new and controversial.

2.7 General Right of Privacy.

A general right of privacy should be extended to the extent possible to the electronic environment. CU and all electronic users should treat electronically stored information in individual files as confidential and private. Contents should be examined or disclosed only when authorized by the owner, approved by an appropriate institution official, or required by law. Privacy is mitigated by the following circumstances.

a. CU is an agency of the State of Oklahoma and therefore subject to the Oklahoma Public Records Act. For CU employees, electronic information created in the performance of their duties may be public records, just as are paper records. Such records may be subject to review and/or release under Oklahoma law. All computer files and e-mail communications, unless subject to a specific privilege, are subject to production under the Oklahoma Public Records Act and, when relevant, to discovery in civil litigation. In these cases, disclosure of personal e-mail or files not related to the specific issue discussed in any Public Records request or discovery will be avoided to the extent allowed by law.

b. Administrative files of CU are generated as part of the process of managing the institution. Files that employees create or maintain can be reviewed by supervisors within this administrative context. Generally, faculty research files and files relating to scholarly endeavor will not be subject to such a review.

c. There is an acknowledged trade-off between the right of privacy of a user and the need of system administrators to gather necessary information to ensure the continued functioning of these resources. In the normal course of system administration, system administrators may monitor any computing activity or examine activities, files, electronic mail, and printer listings to gather sufficient information to diagnose and correct problems with system software or hardware. Sometimes system administrators may monitor computing activity or access files to determine if security violations have occurred or are occurring. In that event, the user should be notified as soon as practical. System administrators at all times have an obligation to maintain the privacy of a user's files, electronic mail, and activity logs.

d. Computer systems and stored data are subject to review by authorized personnel for audit purposes or when a violation of CU policy or law is suspected.

2.8 Disclaimer – CU makes no warranties of any kind, whether express or implied, regarding the electronic communications facilities or services it provides. CU will not be responsible for any damages suffered by a user through the use of the CU electronic communications facilities or services, including, but not limited to, loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or by any error or omissions or any user. Use of any information obtained via the Internet will be at the user's risk. CU specifically denies any responsibility for the accuracy or quality of information obtained through its electronic communications facilities and services.

3.0 Procedures

3.1. Computer accounts will be issued to authorized users only by Information Technology Services personnel.

3.2. Prior to issuance of an account and password, all users must execute such forms, including an acknowledgment and acceptance of the terms of this policy, as may be reasonably required by

CU.

3.3. User passwords must be kept private, and may not be disclosed to any other individual or entity. Passwords should be memorized; however, if a password is written down, it must be kept at all times in the user's wallet or purse. A password must NEVER be posted or placed where it can be discovered by someone other than the user.

3.4. Each user will be assigned a Userid in accordance with rules established by Information Technology Services. The Userid will be used consistently for all logons.

3.5. Personal passwords will be maintained by the individual user and must be changed at least every 90 days for faculty and staff and at least every 120 days for students, or at more frequent intervals as the user may elect. Passwords shall be selected in accordance with rules established by Information Technology Services. In the event another person learns a user's password, the user must immediately change the password. Information Technology Services will never ask a user for their password.

3.6. Any user who learns of an unauthorized use of his or her account must report the unauthorized use to Information Technology Services immediately.

3.7. In the event it appears that a user has abused or is abusing his or her computing privileges, or engages in any misuse of computing resources, then CU may pursue any or all of the following steps to protect the user community:

a. take action to protect the system(s), user jobs, and user files from damage;
b. begin an investigation, and notify the suspected abuser's project director, instructor, academic advisor, dean or administrative officer of the investigation;
c. refer the matter for processing through the appropriate CU disciplinary system;
d. suspend or restrict the suspected abuser's computing privileges during the investigation and disciplinary processing. A user may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the procedures existing at the time the user requests an appeal, which procedures will be provided to the appealing user in writing;
e. inspect the alleged abuser's files, diskettes, and/or tapes. System administrators must have reasonable cause to believe that the trail of evidence leads to the user's computing activities or computing files before inspecting any user's files;
f. In the event the misuse also constitutes a violation of any applicable federal, state or local law, CU will refer the matter to appropriate law enforcement authorities.

Contacts

Policy Questions: Information Technology Services Office, (580) 581-2255

Forms

In support of this policy, the following forms are included:
Faculty and Staff Mobile Email Agreement (F11)

Policy History

Policy

Issue Date:	April 1996
Reviewed, no revision:	February 2016
	September 2019
Revised:	June 3, 2009
	March 21, 2012
	November 4, 2014