CAMERON UNIVERSITY
Computer Use Policy

Policy Statement

[illegible]

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 bs.edctlnumrmation availab-t -[(an)-4 (d)]TJ -6 9-2 1w 0.40 0.004 Tonk63

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,

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

2.7 General Right ofPrivacy.

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 History

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