

Section	<b>Information Resource Security Policies</b>	04/01/2004	-Effective
Policy	1.010.0 <b>Acceptable Use Policy</b>	11/10/2006	-Revised
		CIS	-Author

## Acceptable Use Policy

### Introduction

Computers, networks, and electronic information systems are essential resources for accomplishing Texas A&M University-Kingsville's mission of instruction, research, and public service. The University grants members of the University community shared access to these resources in support of accomplishing the University's mission. Under the provisions of the Information Resources Management Act, these Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources.

### Purpose

The purpose of this Acceptable Use policy is to establish rules that:

- Ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- Establish prudent and acceptable practices regarding the use of information resources.
- Educate individuals who may use information resources with respect to their responsibilities associated with such use.

### Audience

The Texas A&M University-Kingsville Acceptable Use policy applies equally to all individuals granted access privileges to any Texas A&M University-Kingsville Information Resources.

### Ownership of Electronic Files

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of Texas A&M University-Kingsville are the property of Texas A&M University-Kingsville.

### Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of Texas A&M University-Kingsville are not private and may be accessed by Texas A&M University-Kingsville CIS employees at any time without knowledge of the Information Resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

### Information Resource Acceptable Use Policy

- Users must report any weaknesses in Texas A&M University-Kingsville computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on Texas A&M University-Kingsville systems for which they do not have authorization or explicit consent.
- Users must not share their Texas A&M University-Kingsville account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes. Users must not make unauthorized copies of copyrighted software.
- Users must not use non-standard shareware or freeware software without Texas A&M University-Kingsville CIS approval unless it is on the Texas A&M University-Kingsville standard software list.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized Texas A&M University-Kingsville user access to a Texas A&M University-Kingsville resource; obtain extra resources beyond those allocated; or circumvent Texas A&M University-Kingsville computer security measures.
- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Texas A&M University-Kingsville users

Section	<b>Information Resource Security Policies</b>	04/01/2004	-Effective
Policy	1.010.0 <b>Acceptable Use Policy</b>	11/10/2006 CIS	-Revised -Author

must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on Texas A&M University-Kingsville Information Resources.

- Texas A&M University-Kingsville Information Resources must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material which Texas A&M University-Kingsville may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the Texas A&M University-Kingsville official processes for dealing with academic ethical issues).
- Access to the Internet from a Texas A&M University-Kingsville owned, home based or portable computer must adhere to all the same policies that apply to use from within Texas A&M University-Kingsville facilities. Employees must not allow family members or other non-employees to access Texas A&M University-Kingsville computer systems or networks.
- Users must not otherwise engage in acts against the aims and purposes of Texas A&M University-Kingsville as specified in its governing documents or in rules, regulations and procedures adopted from time to time.
- Users must not engage in the downloading, uploading child pornography, or other unauthorized distribution of copyrighted materials.
- Users will not install wireless access points, routers, or switches on the network. Users are not authorized in any way to install additional network equipment without the express written consent of the Computing and Information Services (CIS) Department. The detection of more than one MAC address per port may result in network deactivation.
- As a state agency, Texas A&M University-Kingsville prohibits the installation and/or use of any P2P software on University owned computers or any computer connected to any Texas A&M University-Kingsville owned network. This is an extension of the State of Texas Executive Order RP58 which prohibits unauthorized or illegal use of peer-to-peer software programs.

#### **Texas A&M University-Kingsville Residential Network (TAMUK ResNet) Policy**

- Students must understand and comply with the Acceptable Use Policy, Internet Usage Policy, Network Access Policy, and Virus Policy. Students of Texas A&M University-Kingsville should understand that although the Residence Hall Internet connection (TAMUK ResNet) is a State of Texas regulated network, all of the same rules of the acceptable use policy apply as if your data were on the primary Texas A&M University-Kingsville network. For further information on CIS computer usage policies please go to <http://www.cis.tamuk.edu/help/policies/policies.asp?nb=HELP>.
- Students must understand and comply with copyright policies and copyright laws. <http://www.copyright.gov/laws/>
- All computers must have anti-virus software installed and currently updated. All computers connected to the network are required to have some form of anti-virus software. Texas A&M University-Kingsville students are authorized to install McAfee anti-virus software free of charge. You can download the software from the CIS website at <http://www.cis.tamuk.edu/download/mcafee.asp?nb=DOWNLOAD&stat=stat02>.
- Operating system software patches need to be current. Students are required to maintain all applicable security and vulnerability patches on their systems. Systems that are found vulnerable or un-patched may be denied access to the network until appropriate corrective action has taken place.
- Students will not install wireless access points, routers, or switches on the network. Students are not authorized in any way to install additional network equipment without the express written consent of the Computing and Information Services (CIS) Department. The detection of more than one MAC address per port may result in network deactivation.
- Users of the TAMUK ResNet are issued network addresses through the use of DHCP. Students will not manually assign IP addresses. Students needing static IP addresses for network gaming or other special requirements may request a static IP address from the CMA helpdesk. Static IP addresses will be good through the semester.
- As a state agency, Texas A&M University-Kingsville prohibits the installation and/or use of any

Section	<b>Information Resource Security Policies</b>	04/01/2004	-Effective
Policy	1.010.0 <b>Acceptable Use Policy</b>	11/10/2006	-Revised
		CIS	-Author

P2P software on University owned computers or any computer connected to any Texas A&M University-Kingsville owned network. This is an extension of the State of Texas Executive Order RP58 which prohibits unauthorized or illegal use of peer-to-peer software programs.

- Students will not operate servers of any type without written approval from CIS. Students are authorized access to the network only as a client. Operation of any server or services such as but not limited to P2P (peer to peer), ftp, web, email, DNS, DHCP, time, etc is prohibited and discovery of servers or services may result in deactivation of network access.
- The TAMUK ResNet will require network logon in order to provide highest network security. Students will be required to use their university provided user ID and password to access the network. A maximum of two simultaneous logons per user ID will be allowed. Exceptions may be granted on a case by case basis. Students requiring additional logons must request in writing through the ResNet Director.

### **Incidental Use**

As a convenience to the Texas A&M University-Kingsville user community, incidental use of Information Resources is permitted. The following restrictions apply:

- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to Texas A&M University-Kingsville approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to Texas A&M University-Kingsville.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, Texas A&M University-Kingsville.
- Storage of personal email messages, voice messages, files and documents within Texas A&M University-Kingsville's Information Resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on Texas A&M University-Kingsville Information Resources are owned by Texas A&M University-Kingsville, may be subject to open records requests, and may be accessed in accordance with this policy.

### **Computer Laboratory General Usage Rules**

Use of any university computer facilities shall be in accordance with the following:

- A valid Texas A&M University-Kingsville identification card must be presented to use any of the lab resources. Only the faculty, staff and students of Texas A&M University-Kingsville are allowed to use these facilities unless other arrangements have been made through CIS and/or the respective department.
- The usage of chat (IRC) programs or playing of games is NOT permitted. The resources in this laboratory may be used only for work that is part of an assigned academic program, official university business or university approved research. All other use is prohibited.
- The installation of personal or other software is not permitted. This is a public (to university users) facility used by many disciplines on campus. As such, these systems have been prepared (with the appropriate hardware and software) to meet the teaching and research needs of the campus users and cannot be used for software or hardware experimentation.
- These are state-owned facilities. The equipment and software in these labs are the property of the state of Texas and its citizens. They are intended solely for the purpose of supporting the educational mission of Texas A&M University-Kingsville. Abuse, misuse, theft, security and other violations are subject to criminal charges.
- Routine, scheduled maintenance is performed on these systems. Routine maintenance of these systems throughout the academic year may cause some of the resources to be unavailable. While every attempt will be made to minimize these outages, scheduling and facility requirements should be done on a timely basis with CIS or the facility's representative to minimize the chance of a system being down at critical times.
- Backup copies of system configurations are maintained by CIS. Backup copies of working system

Section	<b>Information Resource Security Policies</b>	04/01/2004	-Effective
Policy	1.010.0 <b>Acceptable Use Policy</b>	11/10/2006	-Revised
		CIS	-Author

configurations are maintained at other locations by CIS. If a system fails, the backup copy of software is loaded to a “cleaned” system without attempting to recover data or programs not included in the backup configuration. If you need additional software or hardware installed on any of these systems AND wish it included on backups, please contact CIS. The use of personally-owned peripherals such as external storage devices, CD-ROMs, and printers is not permitted.

### **Internet User Guidelines**

The guidelines include, but are not limited to, World Wide Web, Netscape, Explorer and Telnet. These guidelines have been created to define what Texas A&M University-Kingsville considers responsible and ethical behavior. These guidelines apply to all Texas A&M University-Kingsville students, faculty and staff using the campus information resources.

- Internet activities and procedures must be consistent with the university’s academic; computer and Internet use ethics policies as well as federal and state computer crime statutes.
- Texas A&M University-Kingsville reserves the right to monitor, filter and/or review, at any time, all Internet utilization via the university’s Internet access. The university further reserves the right to reveal any Internet access related information to any party that it deems appropriate. The use of encryption, the labeling of a communication as private, the deletion of a communication or any other such process or action, shall not diminish the university’s rights in any manner.
- The university will disclose Internet access information to any party that it may be required to by law or regulation. This may include law enforcement search warrants and discovery requests in civil litigation. For more information refer to the online version.

### **Disciplinary Actions**

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Texas A&M University-Kingsville Information Resources access privileges, civil, and criminal prosecution.