29.01.99.K1.010 Acceptable Use Standard Administrative Procedure

Effective: April 1st, 2004
Revised: April 25th, 2013
Revised: March 28th, 2019
Next Scheduled Review: March 2024

Introduction

Computers, networks, and electronic information systems are essential resources for accomplishing Texas A&M University-Kingsville's (TAMUK) mission of instruction, research, and public service. The University grants members of the University community access to these resources in support of the University's mission. Under the provisions of the Information Resources Management Act (TEX.GOV'T CODE § 2054), these information resources are strategic assets of the State of Texas that must be managed as valuable state resources.

Purpose

The purpose of this procedure is to establish rules that:

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

Audience

This procedure applies to individuals granted access to any TAMUK Information Resource.

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 TAMUK are the property of TAMUK. This statement refers to the actual physical files and not to any intellectual property rights that may be granted to the creators by virtue of other University or System policies, rules, or procedures.

Privacy

Information sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of TAMUK is not private and may be accessed by TAMUK iTech employees at any time without knowledge of the information resources user or owner. Electronic content and systems may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

Acceptable Use Procedure

1. Users must report any incidents of possible misuse or violation of this procedure to the Information Security Officer (ISO).
2. Users must not attempt to access any data or programs contained on TAMUK systems for which they do not have authorization or explicit consent.
3. Users must not share their TAMUK account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorizations purposes.
4. Uses must not engage in the unauthorized downloading, copying or distribution of copyrighted software or materials and must adhere to all copyright policies and copyright laws.
5. Users must not engage in the viewing, downloading or uploading of child pornography.
6. Users must not use non-standard software without TAMUK iTech approval.
7. Users must not engage in activities that may harass, threaten or abuse others, degrade the performance or information resources, deprive an authorized TAMUK user access to a TAMUK resource, obtain extra resources beyond those allocated, or circumvent TAMUK computer security measures.
8. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system.
9. Users must not use TAMUK Information Resources for personal or political benefit.
10. Users must not intentionally access, create, store or transmit material which TAMUK may deem to be offensive, indecent or obscene other than in the course of academic research where it has explicit approval of TAMUK.
11. Users must not engage in activities detrimental to TAMUK.
12. Users of any university information resources must follow all Rules, SAPs and Standards.
13. Users will not install wireless access points, routers, hubs or switches on the network. Users are not authorized to install additional network equipment without the express written consent of the iTech Department. The detection of more than one MAC address per network switch port may result in deactivation of the port.

14. Users are authorized access to the network only as a client. Operation of any server or services such as DHCP, DNS, FTP, web, mail, time, etc is prohibited without the express written consent of the iTech department. Discovery of unauthorized servers or services may result in deactivation of network access.
15. Operating system software must be kept current with the latest service patches and security updates. Systems that are found vulnerable or un-patched may be denied access to the network until appropriate corrective action has taken place.
16. All computers connected to the network are required to have an approved anti-virus software. Installed anti-virus software must be in working order and kept updated with definition files no more than one week old.
17. As a state agency, TAMUK prohibits the installation and/or use of any peer-to-peer (P2P) software on University owned computers or any computer connected to any TAMUK owned network. This is an extension of the State of Texas Executive Order RP58 and the 2008 Higher Education Opportunity Act which prohibits unauthorized or illegal use of P2P software programs.
18. Regardless of the provider, access to the Internet from a TAMUK owned computer must adhere to all the same procedures that apply to use from within TAMUK facilities.
19. Employees must not allow family members or other non-employees to access TAMUK computer systems or networks.
20. Personal computing devices connected to the TAMUK network are subject to this procedure.

Incidental Use

As a convenience to the TAMUK user community, incidental use of information resources is permitted. The following restrictions apply:

1. Incidental personal use of electronic mail, internet access, phones, printers, and other information technology resources is restricted to TAMUK approved users.
2. Incidental use must not result in direct costs to TAMUK.
3. Incidental use must not interfere with the normal performance of an employee’s work duties.
4. No files or documents may be sent or received that may cause legal action against, or embarrassment to, TAMUK.
5. Storage of personal email messages, voice messages, files and documents within TAMUK’s Information Resources should be minimal.
6. Personal messages, files and documents located on TAMUK Information Resources are owned by TAMUK and may be subject to open records requests and/or accessed in accordance with this procedure.

Computer Laboratory General Usage Rules

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

1. A valid TAMUK identification card may be required to use any of the lab resources. Only the faculty, staff and students of TAMUK are allowed to use these facilities unless other arrangements have been made through iTech and/or the respective department.

2. The usage of instant messaging (IM), chat (IRC) programs or playing of games is NOT permitted. The computer lab resources 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.
3. 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. The installation of additional software required by faculty for teaching and student use must be coordinated through iTech.
4. 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 TAMUK. Abuse, misuse, theft, tampering and other violations are subject to criminal charges.
5. 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 iTech or the facility's representative to minimize the chance of a system being down at critical times.
6. Backup copies of the user and department shares of systems are maintained by iTech. If a system fails, a backup copy may be loaded to a "cleaned" system.
7. The use of personally-owned storage devices is not supported.

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract 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 TAMUK Information Resources access privileges, civil, and criminal prosecution

References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
3. Computer Security Act of 1987
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
6. Foreign Corrupt Practices Act of 1977
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas Government Code, Section 441

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404