Appropriate Information Systems Use

Summary

The Columbus State University computer network provides access to resources on and off campus and shall be used in a manner consistent with the instructional, research, and administrative objectives of the University. Such open access is a privilege and imposes responsibilities and obligations. Access to University computing resources is granted subject to University policies, and local, state, and federal laws.

Purpose

The purpose of this policy is to define appropriate use of University computing resources. Appropriate use reflects:

- Academic honesty
- Restraint in the use of shared resources
- Respect for intellectual property, ownership of data, and copyright laws
- Adhering to system security mechanisms
- Protection of individual rights to privacy and to freedom from intimidation and harassment.

All activities inconsistent with these objectives are considered to be inappropriate and may jeopardize continued use of computing facilities.

Policy

The following activities are prohibited:

- Accessing another person’s computer account, files, or other data. Revealing your username and password to another person.
- Using University computing resources to gain unauthorized access to other computer systems.
- Attempting to circumvent or subvert information security measures. Examples include creating or running programs meant to identify security loopholes, to decrypt intentionally secured data, to decode or otherwise obtain passwords or access control information, or to gain unauthorized access to any system.
- Saturating network resources to the exclusion of another's use. Examples include overloading the network with traffic such as large uploads or downloads or malicious (denial of service attack) activities.
- Engaging in any activity that may be purposefully harmful to systems or to any information stored thereon. Examples include creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to university data.

- Unauthorized use of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted audio or video, and the installation of any copyrighted software for which Columbus State University or the end user does not have an active license.
- Viewing offensive material in a public setting. Offensive material generally includes sexually-explicit images and/or text, racist materials, and other hateful commentary. Any material which causes reasonable offense or upset to others is considered offensive.
- Harassing or intimidating others via electronic mail, news groups or web pages. Initiating or forwarding spam (mass unsolicited and unofficial e-mail).
- Forging the identity of a user or machine in an electronic communication.
- Using the University's computing resources for personal gain. For example, selling access to your ID or performing unauthorized work for profit with University resources.
- Performing any act, intentionally or otherwise, that will interfere with the normal operation of computers, peripherals, or networks.
- Engaging in any other activity that does not comply with the general principles presented above.

Users Responsibilities

- Users are responsible for adhering to University policies, and local, state, and federal laws.
- Users are expected to take reasonable precautions to ensure the security of computers and information contained therein. Users must guard against unauthorized viewing of computer screens, unnecessary paper copies of data, unnecessary public discussions of personal information, and other potential sources of information or privacy compromise.
- Users must not, under any circumstances, release any student information to a third party. Disclosure to unauthorized parties violates the Family Educational Rights and Privacy Act (FERPA).
- The H: drive (personal file storage space) must be used responsibly. H: drives are not to be used for applications or materials protected by copyright. Keep in mind that the file servers have a large, but finite, amount of space that is shared by all users. Store only critical, work-related files on your H: drive.
- Passwords should not be written down anywhere that they may be accessible to someone else.
- If a user believes someone else knows or has used their password, they must IMMEDIATELY: (1) Change the password; (2) Report the event to the UITS Help Desk (706-507-8199)
- Users should report policy violations to abuse@columbusstate.edu

Related USG Policy

7.12 Appropriate Use Policy for Information Technology (IT) Resources

Last Update

2/4/14

Responsible Authority

Chief Information Security Officer