Residential Network Acceptable Use Policy

Summary

The Columbus State University residential network (ResNet) provides access to campus resources 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 acceptable use of University computing resources.

Acceptable 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.

Columbus State University reserves the right to:

- configure the network to be efficient and secure for everyone
- monitor network traffic to and from your computer
- deactivate your ResNet connection if necessary
- disable your Novell account only; CougarNet, CougarView and email accounts will remain active

Policy

All users on the ResNet system must read and accept the terms of the following network usage policy.

- Your ResNet connection must not be used to provide email or Internet access to non- students.
- Use of ResNet connections for commercial profit or gain is not allowed in any form other than the publishing of your resume on the World Wide Web. This

includes, but is not limited to, selling access to resources on your computer or making a direct financial gain from use of network resources.

- Your ResNet connection must not be used to provide public access to an FTP server or an HTTP server. In other words, you cannot store web pages or downloadable files on your computer and use your ResNet connection to make them available on the Internet. Also, you cannot be a mirror site for another Internet site. Personal web pages may be stored on CSU's web server by requesting an account.
- The network is a shared resource. Thus, you may not use your ResNet connection to engage in any activity having the tendency to demand a large amount of network resources. This includes but is not limited to Internet telephone use, the downloading of all types of music and video media, online gaming, and Internet-based video cameras.
- You may not attempt to circumvent the ResNet firewall or any other established network services.
- ResNet services and wiring may not be modified or extended beyond the area of their intended use. This applies to all network wiring, hardware and data jacks.
- Your ResNet connection may not be used to transmit any material that can be interpreted as offensive, abusive, or harmful to others.
- Your ResNet connection may not be used to participate in the unauthorized distribution of copyrighted material.
- No users may host any type of server on the CSU campus network. This includes, but is not limited to: Gaming Servers, Torrent Servers, Web Servers, FTP Servers, Mail Servers, Proxy Servers, or Virtual Servers. If a user hosts any type of server on the Columbus State University network, they will be in violation of the Network Usage Policy and could possibly face administrative action.
- All users are responsible for the activity originating from their computer. This includes all actions taken by guests and/or roommates using your computer.
- You may not use your own personal router within the dorm network. Personal routers interfere with our network settings and create problems for other students. If a personal router is discovered on the network, UITS will remove the router from the CSU network. If you need assistance using CSU’s wireless network, please contact the Student Repair Shop to schedule an appointment.

Procedures and 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). http://uits.columbusstate.edu/infosec/laws_regs/security_laws.asp#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 CSU 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:
- Change the password; (2) Users should report policy violations to abuse@columbusstate.edu.

Related USG Policy

3.4 (IT Handbook) Network Services

Last Update

4/17/2014

Responsible Authority

Chief Information Security Officer