

GCSU

Information Security Operational Procedures

ResNet Acceptable Use Policy

OVERVIEW

The Georgia College & State University (GCSU) Division of Information Technology (IT) provides technical support for and monitoring of the GCSU Residence Hall Data Network (ResNet). In cooperation with the Office of Student Affairs, the Office of University Housing and the Office of Public Safety, IT is responsible for ensuring that students abide by the GCSU Residence Hall Data Network Acceptable Use Policy (the Policy.) The Policy shall be enforced in concert with all other GCSU policies, as well as local, state, and federal laws pertaining to the use of the network and computer resources. This document applies to both the GCSU wired and wireless networks.

THE NETWORK ACCESS

The ResNet resources are a state-of-the-art network and every effort is made by IT to provide dependable service. Using load balancing, each student is assigned a level of bandwidth appropriate for authorized use. IT cannot control failure of equipment and/or network and/or remote location problems beyond the boundary of the ResNet. Individuals should always have a contingency plan for critical activities, assignments and/or communications.

DEFINITIONS

Authorized Use: Any scholarly activity, university business activity, or personal activity by an authorized user that does not disrupt the network or violate any law or University policy are considered appropriate areas of use.

Authorized Users: Currently enrolled GCSU students or other individuals as approved by GCSU Chief Information Officer (CIO).

Computing Resources: Refers to and includes any and all forms of computer-related equipment, tools and intellectual property. This includes computer systems, personal computers and computer networks and all forms of software, firmware, operating system software and application software, owned by the University or under the University's possession, custody or control.

ENFORCEMENT OF THE ACCEPTABLE USE POLICY

The purpose of these policies is to assure the availability and quality of service of the ResNet and Internet connections. In most cases, violations will be brought to your attention with a phone call or email message. If the problem is rectified quickly, no further action is necessary. In some extreme cases, it may be necessary to block network connectivity to your computer immediately. For this reason, the IT reserves the right to block network access to/from your machine without warning. Repeat violations may result in permanent loss of network connectivity privileges.

In efforts to keep the network running properly, the network is constantly monitored for abuse. Network data content is never monitored, reviewed or stored. If connections to and from your computer look unusual, you will receive an email or phone call from a network administrator about the activity and be asked to ensure that your computer is configured correctly and/or not infected with a virus. In some cases, you may be asked to modify your activity. In emergency cases your computer may be disconnected from the network without warning.

Failure to abide by the GCSU Residence Hall Data Network and Computer Resources Acceptable Use Policy may result in actions including but not limited to:

- Immediate disconnection from the network without warning
- Disciplinary Action as outlined in University Housing and Student Affairs Policies
- Legal action under state and federal law

Warning about MP3 and Movie Files: Many students are copying and illegally distributing copyrighted materials using protocols including, but not limited to, *.mp3, *.mov, *.ram, and *.wmv. This activity may be considered against federal copyright laws and could result in arrest and prosecution in a criminal case or being sued in a civil case. GCSU in no way condones or encourages this activity and will take action to terminate Residential Network privileges of any ResNet student breaking University regulations, State law and/or Federal laws. The University may also be obliged to cooperate with any criminal investigation regarding these matters. According to copyright law, an individual does not need to be making a profit to be prosecuted for distributing copyrighted materials such as MP3 files or movies. The University has received a number of complaints from the Recording Industry Association of America ([RIAA](#)) about machines that were unlawfully distributing files.

RESNET USAGE POLICY

RESPONSIBILITIES

1. You are responsible for registering your networked game system (Xbox, Playstation III, etc) at <http://service.gcsu.edu/toys.html>. If your registration information changes, please contact the SERVE Help Desk with the updated information.
2. You are responsible for all network traffic generated by your computer. You will be held accountable for violations of the applicable policies regardless of whether you:
 - a) generated the traffic,
 - b) are aware of the traffic or
 - c) are aware of the policy violation.
3. You are responsible to seek clarification from the SERVE Help Desk about any situations that you feel may violate policy.
4. You are responsible for installing, maintaining and utilizing a recognized *Virus Prevention Application* such as McAfee or Norton.
5. You are responsible for protecting the wireless network's security software so it is not transferred from your machine to another. You are also responsible for safekeeping of your authentication user id and password.

RESNET ACCEPTABLE USE POLICY

The performance of normal GCSU business, research, education and other vital functions is dependent upon the appropriate use of network. Any disruption of the network can penalize hundreds of students. To minimize network disruption, the conditions listed below are **strictly prohibited**:

- Any action that would impair the function of the network. This includes intentional or unintentional actions that affect the overall performance of the network.
- Any intentional or unintentional action that would deny or impair network service to another system or user.
- Operation of any server on the network. This includes, but is not limited to:
 - Peer-to-Peer programs that share music, video or other files.
 - Hosting a WEB site on a machine connected to the ResNet.
- Any action that violates Federal, State or University policy or law.
- Providing access to the University network to non authorized users.

- Using a computer, computer account or system (including scanning systems for security loopholes, user accounts, passwords, etc.) without authorization.
- Using the campus network to gain unauthorized access to any computer.
- Connecting to another Internet Service Provider (dial-up, DSL, Cable modem) while connected to the ResNet.
- Knowingly performing an act that will interfere with, damage or otherwise degrade the normal operation of other systems and/or network resources, including but not limited to, running, installing or distributing programs known as computer viruses, Trojan Horses and worms.
- Attempting to monitor or tamper with another individual's electronic communications, including scans, "sniffers" and probes of the ResNet and other networks.
- Attempting to circumvent data protection schemes or security mechanisms.
- Misrepresenting your identity to avoid accountability including, but not limited to:
 - falsifying your e-mail address
 - impersonating others in any communication forum
- Using another individual's computer account identity.
- Violating terms of applicable software licensing agreements or copyright protection laws, including making available materials such as music, videos, text or software without appropriate permission.
- Taking any action that invades the privacy of individuals or entities that are creators, authors, users, or subjects of information resources.
- Using ResNet to violate any State or Federal law or regulation, or the University's Honor Code.
- Using the network for commercial purposes, for personal financial gain, or the exchange of services for money or any other thing of value. Advertising of the availability for sale of miscellaneous used personal property belonging to the resident is not commercial within the meaning of this paragraph.
- Using an unauthorized IP address or statically assigned address without approval.
- Using electronic mail, services, or facilities to harass others, including, but not limited to:
 - Sending unsolicited mass mailings over the network (chain mail, solicitations, etc.)
 - Sending email and/or attachments to an individual that has requested that such email and/or attachments not be sent.
 - Using harassing comments or activities during Internet Chat applications.
- Connecting a personal "Wireless Hub" to the ResNet.
- Extending the ResNet network services. Wiring may not be modified or extended beyond the area of their intended use of one computer per data jack. This applies to all network hardware, computer lab equipment and in-room data jacks.

Information Technology
 Campus Box 050
 Milledgeville, GA 31061-0490
 (478) 445-1196

Revised: 03/16/09