ResNet Policies

- Network connections must be made with a Category 5 patch cable directly between your computer's network interface card and the wall jack. No intervening hubs, switches, routers, wireless access points & wireless routers, or other networking devices may be used.

  Connecting to a high speed network shared by thousands of other personal computers is inherently different from connecting to the Internet at home via an ISP. Management of such a network requires in-depth knowledge of all network equipment attached to the network and control over all services provided. Unauthorized and/or improperly configured network equipment can hide computers causing problems as well as interfere with critical network services such as DHCP, DNS, etc.

- Computers attached to the Residential Network (ResNet) must have all relevant operating system security patches installed. For Windows-based systems these are normally the critical updates found using Windows Update.

  When your computer is continually connected with thousands of others on a network, the potential for security problems rises dramatically. You have a responsibility not only to yourself, but to the campus and Internet communities as well to secure your machine against known threats. Microsoft provides frequent security updates for its Windows-based systems. Updates are normally available before the addressed weakness is actually exploited. Regular updates help lessen the likelihood you'll be affected (or affect the rest of the network) when an attack occurs.

- All computers must be running up-to-date antivirus software.

  Worms and viruses are a fact of life on a network. All computers must be prepared to repel them with antivirus software. Since new viruses appear daily, it is imperative that you keep your antivirus software updated to make it aware of the newest threats. Failure to do so can result in total loss of information on your computer as well as disruption of the campus network.

- Your Southeast Key (SE Key) must be used to obtain an IP address once your computer is attached to ResNet. No hard coded IP addresses are permitted without prior approval of Information Technology.

  When you first attach your computer to ResNet and launch its web browser, you'll be taken to a web page to register your computer on the network. After entering your SE Key and associated password, a unique Internet address will be assigned to your machine. Your computer will automatically renew this address from time-to-time, at which point the address might change. If you manually configure your computer with an Internet address, you will quite likely wind up duplicating an address that has already been assigned to another computer, causing both not to work.

- No computer may act as a server on ResNet. This includes web servers, ftp servers, file sharing (e.g., Kazza, Morpheus), etc.

  Heavily used servers place an undue burden on networking resources. This is especially true of those accessed via our Internet connection. Peer-to-peer file sharing systems, such as those used by music and video services, are often problematic because of the heavy use they receive from external users.

- No part of a computer (files, hard drive, or peripheral devices such as printers) may be shared between machines on ResNet.

Worms often spread from machine to machine via open (improperly secured) shares on a network. Intruders use them to gain access to your machine. Increased levels of traffic also result from the advertising of the shares.

- Only the TCP/IP protocol may be used on ResNet.

  Only the TCP/IP protocol is required. Other protocols, such as IPX/SPX and AppleTalk should not be installed on computers attached to ResNet.

- Information Technology is charged with maintaining security and managing bandwidth on ResNet. If a problem can be isolated to a particular port, that port will be deactivated. Due to the automation of this process, we will be unable to notify those affected. From time to time it might be necessary to disconnect entire floors or buildings to locate the source of a problem.

  Surprising as it might seem, it's possible for one compromised computer or improperly configured piece of networking gear to affect the operation of an entire network. When network communications are affected, the only remaining means of troubleshooting is often to disconnect various parts of the network until the problem is isolated.

- The use of packet sniffing software and/or hardware is prohibited.

  Snooping on network traffic will be considered an attempt to violate network security.

- Information Technology will not perform Network Interface Card installs, hardware repairs or software maintenance on student computers.

  Information Technology does not have the staffing required to perform repairs on students' computers. If assistance is needed, it might be necessary to contact an external vendor to obtain the necessary services.

- Information Technology will assist students in making a connection to ResNet. If a problem can't be resolved over the telephone, assistance will be provided in-room or via carry in at Information Technology's discretion.

  Most problems encountered during the initial connection to ResNet involve patch cord and software configuration issues. Many of these issues can be handled over the telephone. If a problem cannot be resolved or a hardware problem is suspected, it might be necessary to contact an external vendor for assistance.

- Information Technology personnel may enter student rooms while the student is present or when accompanied by a Residence Life staff member to perform troubleshooting activities or to locate unauthorized networking devices that are disrupting the network.

  Information Technology staff members will not enter or remain in a student's room unaccompanied by the occupant or a Residence Life staff member. While an IT staff member is present, the door to the room should remain open. Please make sure you will be able to stay in your room for a reasonable length of time when scheduling a service visit with the Help Desk.

- Traffic on ResNet is subject to prioritization at Information Technology's discretion to insure bandwidth availability for academically related activities.

The campus network, including ResNet, is to be used in support of the University's academic mission. To this end, Information Technology uses traffic prioritization in conjunction with quality of service mechanisms to provide the best possible throughput for traffic such as web browsing, e-mail, Mobius and interactive video.

- Firewalls may be used by Information Technology to protect network resources. Both traffic prioritization and firewalling may have negative impacts on some types of traffic.

  From time-to-time it is necessary to control access to certain network protocols and/or ports for security or performance reasons. During periods of heavy network traffic, some protocols such as those used by peer-to-peer file sharing services and network-based games may be blocked or set to such low priority that they appear to be blocked.

- The University e-mail system (using SE Keys) and the University telephone system will be the primary methods of contact regarding ResNet issues. Failure to reply to a request for information may result in temporary disconnection from the network if such action is deemed necessary to protect network services.

  If it becomes necessary to contact you regarding a network issue (such as a virus infecting your computer) Information Technology will attempt to e-mail you using your SE Key and/or call you at the residence hall number listed on your student record.

- Violation of ResNet policies or Southeast's Computing policies may result in disconnection from ResNet. Violators will be referred to the Dean of Student's for possible disciplinary action.

  Most violations are unintentional and can be easily corrected by responding promptly to notifications from Information Technology.

(Revised 2/5/04)