INTENT

The computing, network, and telecommunications resources of Edinboro University of Pennsylvania are intended to support instruction, administration, research, development, and, in general, to advance the overall goals of the institution.

DEFINITIONS

a. Technology and Communications – organizational unit of the University; reports to the President through the Associate Vice President for Technology and Communications. This unit is responsible for campus-wide information systems; desktop and lab computing; learning technologies; and data, video and voice communications.

b. User – any individual provided with access to the described resources.

c. EUPnet – the combination of voice, video and data networks of the University, with the exception of Resnet. Since EUPnet is critical for transacting the business of the University, including conducting classes, handling finances, and serving students, it is designated as the University’s production network.

d. Resnet – the voice, video and data networks of the residence halls.

e. Banner – integrated information system software licensed to the University by SCT Corporation; the main database of the University.

f. SCOTS – Student Centered Online Transaction System; provides an individual with access using the Web to their own data stored in Banner.

g. Authentication – ensures an identity. Each ID requires a technique for validating identity such as a password or a Personal Identification Number (PIN).

h. Virtual Private Network (VPN) – way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization’s network. Edinboro University has a VPN service that can be accessed through a person’s home Internet Service. A user must be authenticated to use this service.
i. Peer-to-Peer (referred to as P2P) – type of Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another’s hard drives. Napster and Gnutella are examples of this kind of peer-to-peer software.

j. Remote Access – the ability to get access to a computer or a company network from a remote distance. People at branch offices, telecommuters, and people who are traveling can get access to the corporation’s network. The University’s remote access consists of dial-up connections through desktop, notebook, or handheld computer modems over regular telephone lines.

**PROPER AND AUTHORIZED ACCESS TO COMPUTERS AND SYSTEMS**

All students, faculty, and staff are eligible for access to general purpose computing and network resources, provided established procedures and regulations are followed. Access is provided in the form of EUPnet, email, and SCOTS accounts. To become a valid student user, one must be a currently registered student. Accounts are maintained over the summer break period unless the student graduates or is not enrolled.

Faculty and staff members are provided EUPnet, email, and SCOTS accounts upon their employment. Banner access is assigned to employees by the Banner security officers depending upon the employee’s role within the University.

External parties may request guest EUPnet and email accounts through Technology and Communications; such access is limited based on availability of resources and its relation to the mission of the University. Participants of special approved programs may be eligible for accounts through permission obtained by the University employee organizing the project.

An individual shall only use the account that was assigned to him/her. A user may not provide their password to others, and must take reasonable steps to ensure its security. Additional requirements regarding access and security are covered under the Information Security Policy for Administrative Information.

**ACCEPTABLE ACCESS TO EUPnet**

Request for a New Connection: Anyone wishing to have a device connected to the network must contact the Help Desk. No device may be connected until after an appropriate network name and address has been assigned.

Termination of Connection: Technology and Communications must be informed before equipment is removed from the network to ensure that network addresses are reclaimed and that cabling is left in a proper state.
Change or Relocation of Equipment: Technology and Communications must be informed before equipment is moved to a different location or equipment is to be replaced by something different than that which was registered for that connection.

Unauthenticated Users: Full network access is only provided to authenticated users. A networked device that does not demand any form of Edinboro University centralized user identification will not be permitted to have direct access to the network. Devices must not transmit "unauthenticated user" traffic via network resources. EUPnet provides means to allow for privately owned PCs to access network resources for both wired and wireless connections by a special authentication procedure.

Remote Access and VPN (Virtual Private Network) Services: To provide access to EUPnet from off-campus locations, Remote Dial-in and VPN services are provided by Technology and Communications to allow authenticated access to EUPnet by staff and faculty.

Wireless Network Access: Wireless 802.11b network access is provided in several campus buildings including the Baron-Forness Library. All wireless devices will be required to provide authentication upon establishing a connection.

Network Power: Many buildings serve as network connection points for other buildings on the campus. Technology and Communications must be contacted before power is interrupted to any building or satellite equipment room housing network equipment.

Peer-to-peer file sharing applications will not be available on EUPnet in order to reduce illegal distribution of copyrighted material (music, videos, etc.). Students and employees who have a legitimate educational or research need for these applications should contact their dean or vice president for permission, who will then submit their request to Technology and Communications to turn on access for that individual for a specified time period.

COMMUNITY RESPONSIBILITIES

All users are bound by this policy and have the responsibility of ensuring that their utilization of computing resources is consistent with the intent of this policy.

Technology and Communications provides operational responsibility for EUPnet, including the planning, design, installation, problem resolution, and general operation of the network and its associated communication facilities. All network traffic and usage must be in compliance with this policy, procedures, and conditions. Any network traffic exiting the University is subject to the acceptable use policies of the network through which it flows, such as SSHEnet, as well as the policies listed here.

Technology and Communications should be notified about violations of laws and policies governing information use, intellectual property rights, or copyrights, as well as about potential loopholes in the security of its computer systems and networks. The
user community is expected to cooperate with Technology and Communications in its
operation of computer systems and networks as well as in the investigation of misuse or
abuse. Should the security of a computer system or information network be threatened,
suspected user files may be examined under the direction of the Associate Vice
President for Technology and Communications, in consultation with the President.

Misuse or improper practices associated with computing, networks, and
telecommunications include (but are not limited to) the following:

- Attempting to disguise the identity of the account or computer being used
- Use of EUPnet to gain or attempt to gain unauthorized access to remote
  computers
- Any deliberate act which may seriously impact the operation of computers,
  peripherals, or EUPnet. Such acts include, but are not limited to tampering with
  components of a network, blocking communications lines, interfering with the
  operational readiness of a computer, creating or altering device names, subnet
  masks or IP addresses
- Placing a device in promiscuous mode, or using a program that places a device in
  promiscuous mode, for the purpose of capturing and monitoring network packets
  without the expressed permission of Technology and Communications
- Installation of unauthorized network hubs, switches or routers including wireless
  access points
- Running or installing programs which could result in the eventual damage or
  disruption of files, computers, or networks
  This is directed toward, but not limited to, classes of programs known as viruses,
  Trojan horses, and worms.
- Frivolous use of the computer (i.e. - use of entertainment software for non-
  educational or non-productive reasons, sending mail or messages without an
  appropriate reason, printing an unnecessary amount of paper output, circulation of
  chain e-mail)
- Use, modification or inspection of programs, data or functions which are neither
  allotted nor authorized to the user's account, nor specified as public
- Use of another's account or the distribution of your account password to another
  user or to those not authorized to use the system
- Physical or electronic interference with other users of the system
- Sending messages, naming files, or programs with obscene or vulgar language
- Copying copyrighted materials or making them available for others to copy without
  the appropriate expressed written permission of the copyright holder
  Furthermore, the copying of site-licensed software for distribution to persons other
  than Edinboro University faculty, staff, or students, or the copying of site-licensed
  software for use at locations not covered under the terms of the license agreement,
  is prohibited.
- Any other practices or procedures which, in the opinion of the supervisory
  personnel of Technology and Communications, and/or management of Edinboro
  University of Pennsylvania, promote illegal activities or constitute a misuse of any
  University computer facilities or resources, or otherwise jeopardize their operation
PROTECTION OF INFORMATION IN ELECTRONIC COMMUNICATIONS

Beyond the Federal Educational Rights and Privacy Act (FERPA) and employment data, users should not have any expectation of privacy with electronic mail, user accounts, passwords, and computer storage devices. Electronic mail is generally protected from access by other users. However, electronic mail may pass through other systems over which the University has no control. Electronic mail that is incorrectly addressed, or encounters other delivery problems, is normally routed to local postmasters so it can be processed manually. Users are advised to treat electronic communications correspondence with the same formality and expectations with which they would treat written, non-electronic correspondence. Note that deletion of material from a computer system does not necessarily delete it from system backups.

The Federal Electronic Communications Privacy Act puts limitations on the interception of electronic communications. There are some circumstances where reading electronic mail for the purpose of resolving problems is permitted, provided that the contents are not disclosed any further. In some cases where such action leads to a belief that a law has been broken, the contents may be disclosed to the appropriate authorities.

Technology and Communications will log the source and destination of all electronic mail messages for the purpose of network traffic analysis.

With regard to University email distribution lists, senders need to ensure that the messages are appropriate for the intended audiences and are in accordance with the appropriate use requirements of this policy. Messages to distribution lists must be limited to those which announce official University information or a University-sponsored event or activity. Senders are encouraged to take advantage of the Weekly Messenger to distribute campus-wide messages rather than individual messages to the campus community.

NETWORK EQUIPMENT DESIGN AND MANAGEMENT

All new construction and renovation projects must include consultation with Technology and Communications to ensure these projects provide the facilities necessary to install and support satellite equipment rooms and cable raceways for network wiring and interconnecting cables.

All network equipment must be approved by Technology and Communications for use on EUPnet to ensure that centralized management can be sustained, thereby assuring network integrity.

COMPUTER AND NETWORK SECURITY

Connections to external networks such as the Internet make University computer systems vulnerable to break-in attempts from remote systems. These connections also
make University systems susceptible to virus and worm attacks. The University does maintain a central firewall to reduce the risk of break-in attempts and provide additional network security, as well as virus protection software to reduce the threat and spread of computer viruses. All computers are required to have operating virus protection software as provided by Technology and Communications.

Viruses and Worms: All gateways to external networks will be shut down at the first indication of a virus or worm attack. Technology and Communications will contact the CERT (Computer Emergency Response Team) to either confirm or deny the existence of Internet security problems and take action accordingly.

Remote Access: Technology and Communications will log and monitor the source of all remote access attempts including TELNET, FTP, Finger, Talk and Ping requests. No person shall attempt to circumvent data protection schemes or uncover security loopholes.

To ensure continuity in the security plan and its identification as a University asset, any equipment connected to EUPnet must be registered under the edinboro.edu domain and named accordingly.

**TELEPHONY AND VOICEMAIL APPROPRIATE USE**

Residence hall students, faculty and staff are provided local telephone service. Local calls are defined as non-toll calls within the Verizon local service area. Students may place local calls from their residence hall room telephone line. Telephone instruments are the responsibility of the students living in the room.

Faculty and staff may access all University-owned telephone lines and place local calls from their office or departmental telephone. External users are permitted use of the lobby phones to direct dial on-campus extensions.

Access to long distance service is available to residence hall students through the use of a personal calling card using toll-free access numbers. The contracted long distance provider network is available to all faculty personnel. All direct dial long distance calls may be placed from telephones with an unrestricted class of service for University business only. This is accomplished using a long distance authorization ID number provided to every employee. Departments are billed for the long distance charges of their department members. If any non-business calls are inadvertently placed, restitution for them is expected by the individual who made the call.

Other services billed to the departments include additional telephone desk sets and accessories, calling cards, mobile phones and phone service, and inbound toll-free number calls.
All authorized external users utilizing University-owned telephone lines and services are subject to reimburse the University for telecommunication-related expenses associated with those lines.

Student-placed incoming and outgoing calls are not permitted to be billed to University-owned telephone lines. Faculty- and staff-placed incoming and outgoing calls are not permitted to be billed to University-owned telephone lines other than the originating telephone line. Faculty and staff are not permitted to transfer or call-forward calls to non-University owned telephone lines unless IT IS FOR university-related business.

Only FCC compliant telecommunication devices may be attached to University-owned telephone lines.

Many buildings serve as telecommunication connection points for other buildings on the campus. Technology and Communications must be contacted before power is interrupted to any building or satellite equipment room housing telecom equipment.

**ACTIONS RESULTING FROM MISUSE**

Devices not complying with campus EUPnet standards will be immediately disconnected from the network until the device is brought into compliance with established standards. This will be done to prevent disruption of EUPnet services.

Edinboro University of Pennsylvania reserves the right to invoke serious action against a user who willfully misuses computing, network, or telecommunications resources. Users who deliberately misuse EUPnet will be denied access to network facilities. Deliberate and/or negligent abuse of any university resource, including University computer systems and EUPnet, could lead to disciplinary action. For students, such actions may include the filing of charges according to the student Code of Conduct. Bargaining unit members are subject to applicable procedures as defined in their collective bargaining agreement. Staff and other non-bargaining unit employees are subject to actions established by the University. All users are subject to any applicable criminal prosecution according to local, state, and federal laws.