

STATEMENT

The campus data communication network, and the electronic communication systems by which it is interconnected and accessed, exists to support the research, instructional, and administrative needs of California University of Pennsylvania. The network and associated facilities constitute a critical resource. This policy exists to inform the members of the educational community about the manner in which these resources are administered so they will better understand what is expected of them in helping to ensure that the resource provides the best possible service.

POLICY

The Computer Services Center (CSC) provides operational responsibility for the university data communication network, including the planning, design, installation, problem resolution, and general operation of the network and its associated communication facilities.

1. Network Protocols:

Data transmission across the campus backbone is restricted to DECnet and the industry-standard TCP/IP protocol suite. Subnetworks may use other protocols when necessary as long as the subnet is connected to the backbone using a gateway that supports protocol conversion.

2. Network Numbers and Addresses:

The CSC will maintain a registry of all devices operating within the campus network and will assign the appropriate DECnet address, subnet mask, IP host numbers, and node names to each device. The campus network uses a 32-bit class-B IP network number, 158.83.0.0; the 16-bit 0.0 portion is assigned by the CSC; currently an 8-bit subnet number followed by an 8-bit host number.

3. Network Connections:

A. Request for a New Connection:

Anyone wishing to have a device connected to the network must submit a "Campus Network Connection Request" form to the CSC. No device may be connected until after an appropriate network name and address have been assigned.

B. Termination of Connection:

The CSC 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.

C. Change or Relocation of Equipment:

The CSC 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.

D. Untrusted Devices:

Any device that is under control of an individual whom the university is uncertain will operate in the best interests of the university at all times will be defined as "untrusted". An untrusted device will only be attached to a cabling system that contains no trusted devices, and that cabling system will be connected via a router (or other suitable equipment) that is a trusted device. The trusted device should prevent the untrusted device from capturing and analyzing network packets

or aliasing the address of a trusted device.

E. Unauthenticatable Users:

Network access is limited only to "known" users. Devices must not transmit "unauthenticated user" traffic via network resources. A multi-user system is not a concern because each user must have a unique account and password to access the system. On the other hand, a networked device that does not demand any form of user identification can therefore be used by anybody who has physical access to that device. This is not a problem if the device is in an individual's office. However, if the device is in any kind of "common" area, its use cannot be attributed to a specific individual. Such a device will not be permitted to have direct access to the network unless its users must first sign on through an authentication system.

4. Network Wiring:

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

5. Network Power:

Many buildings serve as network connection points for other buildings on the campus. The CSC must be contacted before power is interrupted to any building or satellite equipment room housing network equipment.

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.

1. Viri and Worms:

All gateways to external networks will be shutdown at the first indication of a virus or worm attack. The CSC will contact the CERT (Computer Emergency Response Team) at 412-268-7090 to either confirm or deny the existence of Internet security problems.

2. Remote Access:

The CSC will log and monitor the source of all remote access attempts including TELNET, FTP, Finger, Talk and Ping requests.

NETWORK PRIVACY

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. All California University personnel capable of receiving or accessing undeliverable mail are required to treat this mail as confidential and may not disclose the contents of any mail message. According to the Federal Electronic Privacy Act, interception of electronic communications to enforce a policy or law (absent a warrant) is not permitted. But that under some circumstances, reading mail for the purpose of resolving problems is permitted, provided that the contents are not disclosed, unless a law is found to be

broken, in which case the contents may be disclosed to the appropriate authorities.

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

ACCEPTABLE USE

All network traffic and usage must be in compliance with established university policies, procedures, and conditions, including those of external entities administering resources to which the network or communication facilities are connected.

1. You may not connect or disconnect any device or cable to the campus network without the expressed permission of the CSC. This prevents disruption to network operation.

2. You may not create or alter any device name, Subnet mask, DECnet or IP address attached to the network. Network device names and addresses may only be changed with expressed permission of the CSC.

3. You may not consume bandwidth unnecessarily or deliberately interfere with or impact normal network operations. Some examples include:

- ◆ importing files via FTP from archive servers at other institutions rather than by making use of the local archives when possible
- ◆ subscribing to mailing lists for items that already exist within existing newsgroups
- ◆ issuing (or writing programs that issue) various network interrogation commands like "ping" or "traceroute"
- ◆ participating in "chain letters"

4. You may not place a device in promiscuous mode, or use a program that places a device in promiscuous mode, for the purpose of capturing and monitoring network packets without express permission of the CSC.

5. You may not use the University's resources to gain, or attempt to gain, unauthorized access to local or remote computers. Nor may you provide your account or password to others for the purpose of accessing California's systems.

Employees may, however, provide remote access to any standalone system for which they are responsible, such as a workstation capable of supporting remote access as long as its use is consistent with the intent of this and other University policies, namely research and instruction.

6. You may not use any network resources in support of private activities or personal entertainment without proper approval or making prior arrangements.

ACTIONS RESULTING FROM MISUSE

Devices not complying with campus network 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 network services.

Users who deliberately misuse the network will be denied access to network facilities.

Offenders may also be subject to criminal prosecution. Under Pennsylvania law it is a felony punishable by a fine of up to \$15,000 and imprisonment of up to seven years for any person to access, alter or damage any computer system, network, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization [18 PA.C.S. 3933(a)(1)]. Knowingly and without authorization, disclosing a password to a computer system, network, etc. is a misdemeanor punishable by a fine of up to \$10,000 and imprisonment of up to five years, as is intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software [18 PA.C.S. 3933(a)(2) and (3)].