

V.N. POLICY ON COMPUTER DISCONNECTION FROM PENNNET

(Source: Vice President for Systems and Computing, Almanac, April 20, 1999 (<https://almanac.upenn.edu/archive/v45/n29/communications.html>))

Background: A well functioning network is critical to the research, academic and service missions of the University. Information Security has documented an increasing frequency of computer intrusions that threaten the integrity of PennNet. The capacity of entire departments to teach and conduct research has been limited as a result, and sensitive data have been at risk of unauthorized disclosure. At times, rapid response is required to protect the integrity of systems, data and those that rely on them. Inefficiency sometimes results because the owners of the penetrated machines cannot be located. Disagreements arise over the magnitude and immediacy

of the problems without a formal mechanism for resolving conflicts.

Certain types of misconfiguration of Penn systems, intentional or otherwise, can have serious and detrimental consequences. Examples include using another host's Internet Protocol address ("IP Spoofing") or misconfigured networking protocols. Normal operation of Penn computers, and even computers elsewhere on the worldwide Internet, can be compromised. Networks can become so congested that network traffic cannot get through.

Purpose: The goal of this policy is to prevent disruption of the University's computers and networks.

Policy: Information Systems and Computing (ISC) will disconnect from PennNet any computers that have actually damaged or pose an imminent threat of harming the integrity of PennNet.

Scope: This policy only applies to computers and devices attached directly or indirectly to PennNet, including improper or defective "daisy-chain" connections and private Local Area Networks with active networking components connected to PennNet wall plates and hosts.

This policy does not address removing computers from PennNet for reasons related solely to their content.

Implementation: Systems administrators must report serious computer security incidents to the University Information Security Officer. Serious computer security incidents will be defined as those that jeopardize the integrity, privacy and/or availability of other computers and networks. Examples of serious computer security incidents include break-ins where privileged accounts (e. g. UNIX "root" account, or NT "Administrator" account) are used without authorization, incidents where network traffic is monitored without authorization, and incidents where Penn computers or networks are either the source or the target of "denial of service" attacks. The Information Security Officer shall coordinate the response to computer security incidents, including notifying campus systems administrators, law enforcement officers, external sites, incident response teams and University offices as appropriate.

Authorized actions: If, in the judgment of the Vice President for Information Systems and Computing or his/her designate, a system poses a significant and immediate threat either to the security of other Penn computers and networks, or the continued operation of

Penn networks and computers, and the problem cannot be resolved expeditiously through collaboration between the computer owners and ISC, then ISC shall notify senior management of the department or unit and shall require the owners to remove the computer from the network until the problem is solved.

Absent/Unidentified Owners: If ISC is unable, using the Assignments database, to identify a system owner or Local Support Provider (LSP), ISC will move unilaterally to protect the network by disconnecting the threatening system.

Disputes: In cases where there is persistent disagreement between ISC and the owner of the perceived threat, ISC must notify the owner and the LSP of the following information in writing:

- The reason for the disconnection
- What steps must be taken for the network connection to be restored
- How to arrange for the system to be reconnected
- The process of appealing a decision to disconnect

When the owner of the system has taken the steps necessary to correct the problem, ISC will restore the PennNet connection as soon as possible.

Appealing a Decision to Disconnect: The Council Committee on Communications shall appoint a subcommittee to review appeals of decisions to disconnect computers.

The subcommittee will consist of:

- At least four members of the faculty appointed by the Committee on Communications, one of whom shall serve as chair,
- The Vice President for Information Systems and Computing or his/her designate,
- The University Information Security Officer or his/her designate,
- The Committee on Communications may designate alternates to serve on the hearings of an appeal when its appointees are unavailable.

The owner of a disconnected system who believes that the threat that the system posed is outweighed by the impact of its disconnection on his/her academic mission may appeal the decision by documenting this belief in writing to the chair of the subcommittee. The chair or his/her designate may resolve the dispute amicably; failing this it will be heard formally by the subcommittee. The subcommittee shall resolve conflicts as rapidly as possible within the constraints of fairness. It shall establish and follow its own operating procedures.

If the subcommittee does not begin the proceedings within five working days in cases where the issue is a threat and not actual harm, or thirty working days in cases where ISC can document actual harm, the subject system must be reconnected. Once the subcommittee has begun the process, time limits shall not be imposed.

In considering appeals, the subcommittee shall balance the value of leaving machines connected against the associated risks. Its decision shall be final. The only recourse for faculty whose appeals are denied shall be to the Senate Committee on Academic Freedom and Responsibility. ISC may not appeal. However, it may redisconnect the computer and restart the entire process whenever another trigger event is detected.

System owners who believe that their freedom of expression has been unduly infringed may, under the Guidelines for Open Expression, request

that the Committee on Open Expression determine if the Guidelines were properly interpreted and applied to the disconnection of their system.

For additional information, contact security@isc.upenn.edu.