

# DCTF Policy for the Configuration of Modem Pools

## Background

A modem pool on NYU-NET is defined as a set of one or more modems, attached both to telephone lines and to a device attached to a segment of NYU-NET (e.g. a computer or a terminal server). These include devices to permit access to machines on NYU-NET via networking protocols such as telnet, rlogin, SLIP, PPP, Appletalk Remote, and Novell IPX. The definition encompasses all forms of data modems, and includes CSU/DSUs and ISDN data communications equipment.

There are two types of modem pools: inbound modems (for calls coming into NYU-NET) and outbound modems (for calls leaving NYU). The ACF maintains a central NYU-NET inbound modem pool for NYU community access to campus and Internet-based resources. A small ACF outbound modem pool is used to permit access from NYU-NET-attached computers to external computer systems which are not presently Internet-attached.

Other divisions of the university may have established, or may wish to establish, their own modem pools—either for use solely by a restricted number of staff members for work-related purposes, or for broader use in order to make computer or network resources available to wider audiences.

In addition, an individual on campus has the capability in some cases to attach one or more modems directly to their microcomputer or workstation which may be attached to NYU-NET. Such situations are generally meant for private, individual use of workstation resources from a remote location, and are not intended for public use. This type of modem resource is not a "modem pool" per se, although its configuration and use raise some of the same security issues as true modem pools.

## **Organizations and individuals who set up modem resources must recognize that:**

- Modem-attached phone numbers cannot, in the general case, be kept private or unlisted with absolute certitude, especially in the context of making their use available to communities of users.
- Modem resources therefore represent a set of security and resource allocation/protection issues in the areas of access and security of NYU-NET, the Internet, and NYU telephone access and security.
- The underlying goals in establishing any configuration and management guidelines

for modem resources, then, are: to enable access capabilities for authorized members of the community while preserving good security and privacy of NYU resources, and protecting against access by unauthorized individuals.

## Guidelines

The following guidelines for modem pool configuration and management are set forward by the DCTF:

### Identification of Modem Pools

NYU-NET management must be aware of modem pools on campus:

- Modem pools may only be established and supervised by employees of the University.
- All presently existing modem pools should be identified to the NYU-NET NOC, via electronic mail to [noc@nyu.edu](mailto:noc@nyu.edu). Descriptions should be provided for their current configuration, intended use, community of authorized users, security provisions; the staff members responsible for these systems should be identified.
- All planned modem pools should be similarly identified to the NOC, and NOC staff members should be consulted on configuration and management issues.

### Outbound Modem Pools

Outbound modem pools may **not** be attached to NYU-NET, with the sole exception of the central NYU-NET outbound modem pool configured and maintained by the ACF so as to guarantee a high degree of security for NYU networking and telecommunications resources. Any proposed exception to this rule must be formally approved by the NYU Data Communications Task Force. Access to outbound pools calls for special security provisions, and any new outbound pool would likely be required to implement call logs and password protection.

### Configuration of Inbound Modem Pools

All inbound modem pools attached to NYU-NET are to have the following attributes:

- All modem pools must be owned and controlled by departments or divisions of the University; management functions and responsibility must be assigned to University staff members.
- All users must be authenticated by username/password identification at the point of dial-in (at the terminal server/computer to which the modems are attached). Responsible username/password policies must be used (e.g. passwords must be of a

certain length, must expire at some interval and be changed).

- As a rule, accounts on NYU computer systems (including accounts for modem-pool authentication, should be restricted to members of the New York University community. Exceptions to this policy should be weighed carefully.
- SNMP management capabilities must be present on networking hardware used by the modem pool. The central NYU-NET NOC ([noc@nyu.edu](mailto:noc@nyu.edu)) should be consulted on SNMP configurations issues.
- Call logs must be maintained by the organization responsible for the modem pool.

## **Individually-maintained Modem Resources**

The restrictions described above do not apply to individual data modems attached to microcomputers/workstations by their owners for the purpose of private dialin/dialout use. The DCTF reserves the right, however, in cooperation with NYU Telecommunications, to establish specific rules or restrictions for the configuration and use of individual modems on machines attached to NYU-NET.

All contents copyright

© New York University

All rights reserved

Page last revised: **May 1994**

Page last reviewed: August 22, 2006