

Authenticated NYU-NET Access to the Internet

Organizations participating in the world-wide Internet must provide reliable and secure environments in order for members of their communities to work. The Internet is a cooperative venture in which participants work together to improve capabilities and solve problems.

Unfortunately, all individuals do not wish to abide by accepted conventions of behavior in using the Internet, sometimes violating standards of etiquette, morality, and even law. Examples of such inappropriate practices range from harassing communications, to violations of copyright, to computer system hacking.

In order to identify and locate such individuals, it is necessary to maintain information on components and authorized users of the network. In addition, it is necessary to restrict the degree to which unauthorized or unauthenticated individuals can use local network and Internet resources.

RFC 1173 "Responsibilities of Host and Network Managers" states:

Because Internet security issues may require local management either get in touch with any of their users, or deny an offending individual or group access to other sites, it is necessary that mechanisms exist to allow this. Accordingly, Internet sites should not have "general use" accounts, or "open" (without password) terminal servers that can access the rest of the Internet.

The DCTF therefore prohibits "anonymous" access from NYU-NET to the Internet. This means that persons using NYU-NET resources to access the Internet must either:

- gain access only after providing a uniquely identifying username and password

or

- be using a networked machine registered for their individual use in the Domain Name System (DNS).

It is the responsibility of individual network managers and host system managers to implement this policy and to maintain logs of network and host access. Changes in assigned users of individual networked machines, e.g., through new staff hiring, should be

reported to the NYU-NET Network Operations Center (NOC) in order that the DNS may be updated. Any sign of NYU-NET or Internet abuse must be communicated immediately to the NOC.

Violators of this policy may find their network access disabled, with no prior warning, until sufficient safeguards have been put into place to ensure that no further violations take place. The DCTF reserves the right to disconnect individual machines or sub-networks of NYU-NET in order to preserve the smooth functioning and security of the network as a whole.

It is the responsibility of all network users to accept full responsibility for the use of their accounts and machines, and to preserve their sole individual use of their accounts by not sharing them with other individuals, by maintaining secret passwords, by changing passwords frequently, and by selecting passwords which are difficult to guess or decrypt.

All contents copyright

© New York University

All rights reserved

Page last revised: **February 2, 1995**

Page last reviewed: August 22, 2006