Colorado University of Colorado at Boulder	**CIO Campus-wide Policy**

Effective:	May 2003
Responsible Office:	CIO
Policy Title:	Network Security Policy
Approved	*IT Council*

Purpose: Outlines expectations regarding network traffic, servers, and management.

A. Rationale and Scope of Policy:

The University of Colorado at Boulder (CU-Boulder) provides network services to a large number and variety of users – faculty, staff, students, and external constituencies. Security compromises for any campus-networked system can have a detrimental impact to other networked systems. Information Technology Services (ITS) is the primary information-technology provider on the CU-Boulder campus, with services for telephony, video, computing, and networking. ITS has campus-wide responsibility to maintain the integrity and security of networking systems and to provide the wiring and cabling infrastructures that support voice, data and video services.

This policy encompasses all systems directly connected to ITS-maintained networks or systems on networks that receive network service from the Boulder campus backbone. This includes campus Internet connections, 10BaseT or 100BaseT “b-jack” connections, DSL subscriber lines and “Alliance Networks”.

B. Policy:

1. Network Traffic

ITS will control access to all intra-campus traffic, all inbound and outbound Internet traffic, and DSL service. The ITS Executive Director or his/her designee will determine what Internet traffic will be permitted. IT Council will have a consultative role to ensure that the traffic limitations are consistent with both the business and academic goals of CU-Boulder.

2. Network Servers

All Network Servers must have registered IP Addresses in order to insure that any additions or changes to the Network Servers will not have adverse effects on the existing resources. IP Address registration is available on the ITS web site www.colorado.edu/its/networking.

3. Network Management

The IT Security Office, or its designee, is authorized to perform a security audit of any CU-Boulder network devices at any time.

The IT Security Office is the primary administrative contact for all network security related activities.

All networked systems will comply with the Minimum Security Standards policy.

The IT Security Office will publish security alerts, vulnerability notices and patches, and other pertinent information in an effort to prevent security breaches.

ITS will coordinate investigations into any alleged computer or network security compromises, incidents, and/or problems. To ensure that this coordination is effective, ITS requests that security compromises be reported to ITS (e-mail: security@colorado.edu).

ITS will monitor backbone network traffic in real-time as necessary and appropriate, to detect unauthorized activity or intrusion attempts. All monitoring will be carried out in compliance with the "Use of CU-Boulder's Computing and Network Resources" policy.

If scans or network monitoring identify security vulnerabilities, the cooperation of the system owners and system managers for the systems and the networks will be solicited. If the appropriate contact cannot be determined, the department's management will be notified. When a security problem (or potential security problem) is identified ITS will take steps to disable network access to those systems and/or devices until the problems have been rectified. ITS will disable network access at the closest network port to which ITS has administrative control.

C. Responsible Organization

The CIO Office will be responsible for the maintenance and review of this policy.