Minimum Security Standards for Networked Devices

1. Rationale 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 (IT) provider on the CU-Boulder campus, with services for telephony, video, computing, and networking. ITS, as the primary IT provider, 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

The CU-Boulder encourages the use of its electronic communications network in support of education, research, and public service. However, this resource is limited and vulnerable to attack. CU-Boulder therefore reserves the right to deny access to its electronic communications network by devices that do not meet its standards for security.

This policy requires compliance with minimum security standards to help protect not only the individual device, but other devices connected to the electronic communications network. The policy is also intended to prevent exploitation of campus resources by unauthorized individuals.

2. Policy

Access to and use of campus network services are privileges accorded at the discretion of the CU-Boulder campus. Devices connected to the CU-Boulder electronic communications network must comply with the minimum standards for security set by the Campus IT Security Officer. Devices that host sensitive or critical data are required to conform to more rigorous security standards. Campus departments, units, or service providers may develop stricter standards for themselves. Devices that do not meet minimum standards for networked host security configurations may be disconnected.

3. Scope of Policy

This policy encompasses all systems directly connected to ITS-maintained networks or systems on the Boulder campus backbone.

3.1 Noncompliance

When a system is identified to be an infecting agent ITS will take steps to disable network access to those systems and/or devices until the

problems have been rectified.

4 Responsibility

4.1 Individual

Each individual must ensure that their systems are in compliance with established minimum standards. In the absence of a system administrator the system owner will function as the system administrator.

The system owner will accept responsibilities of the system administrator in the absence of an assigned system administrator.

The system owner will be responsible for ensuring that contracted system administration complies with campus policy and the minimum system standards.

4.2 Information Technology Services

ITS and the IT Security Officer will publish minimum security standards and implementation guidelines in consultation with IT Council. Separate security standards will be established for desktops, servers, web and Internet servers, and other networked devices.

ITS will provide implementation guidelines and when feasible infrastructure to support the implementation and enforcement of the minimum security standards.

5. Procedures

5.1 Process for granting exceptions to the policy

Requests for exceptions should be presented for approval to the Executive Director of ITS or his/her designee.

6. References

2007 CU-Boulder Minimum System Security Standards

CU-Boulder Computing and Network Resource Use Policy document

ITS Network Security Policy

University System “Providing and Using Information Technology” Policy

University System “Adopting Standards and Best Practices for the Acquisition and Deployment of Technology and Ancillary Support Infrastructure” Policy

7. Responsible Organization

The ITS Executive Director and the Campus IT Security Officer will be responsible for the maintenance and review of this policy.