University of Colorado

Information Technology Services

CU-Boulder Minimum System Security Requirements

Table of Contents

1 Introduction

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.

The CU-Boulder Minimum Security Standards for Networked Devices policy requires compliance with minimum security standards detailed in this document 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.

1.1 Policy Reference

CU-Boulder Minimum Security Standards for Networked Devices
CU-Boulder Network Security

2 Minimum System Security Requirements

2.1 Network Device Registration

All campus networked devices must be registered to receive network access. This registration process would require all faculty, staff and students to register their network devices using campus authentication.

2.2 System Configuration

- OS version must be one for which the vendor is actively providing patches
- The system should only be running Network services required for University academic, administrative, or research functions.
- DHCP Client systems should be on networks behind NAT provided by ITS
- Care should be taken to change insecure vendor defaults for all networked devices. For example, disabling telnet on printers or network hardware or disabling ftp for a web server.

2.3 Software patch updates

Campus networked devices and services running on those devices must have current security patches applied . While ITS sends notices for supported operating systems and a few select applications it is important that those who manage systems monitor and evaluate vendor security notices and apply software updates or patches in compliance with established patch levels. ITS has defined the following categories to describe the severity of vulnerabilities and required patch levels:

- Urgent: represents a broad threat to the entire campus community for which patches must be applied within one business day.
- Severe: includes remotely exploitable vulnerabilities and must be patched within 48 hours.
- Important: includes local exploits and must be patched within one week.

Exceptions may be made by the ITS Security Officer for patches that compromise the usability of critical applications and where other security measures are in place, such as an ITS-supported firewall.

2.4 Anti-virus and Anti-spyware software

Appropriate anti-virus and anti-spyware software must be running and updated daily on networked device, including clients, file servers, mail servers, and other types of campus computers.

2.5 Access Control: Passwords and encryption

All campus IT service providers must use encrypted authentication for password processing. Use of secure protocols in favor of unencrypted protocols (e.g., using SSH rather than Telnet and FTP) is strongly encouraged.

2.6 Physical security

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this all network devices must be configured to "lock" and require a user to re-authenticate if left unattended.

Locate servers in a dedicated room with appropriate physical controls such as a lock or card access system.

2.7 Host-based firewall software

Host-based firewall software (or its technical equivalent such as IPSec, TCP wrappers, hardware firewalls) is required for servers, laptops, and desktops. Care should be taken to ensure that other networked devices (network stitches, printers, web cameras) are not running unnecessary services and when possible only allow access to authorized clients.

2.8 No unauthenticated email relays

Campus devices must not provide an active SMTP service that allows unauthorized third parties to relay email messages, i.e., to process an e-mail message where neither the sender nor the recipient is a local user. Before transmitting email to a non-local address, the sender must authenticate with the SMTP service. Authenticating the machine (e.g. IP address/domain name) rather than the sender is not sufficient to meet this standard. Only campus email gateways (supported by ITS) may accept unauthorized email for relay.

2.9 No unauthorized DNS servers

All DNS servers must be authorized by the campus IT Security Office.