Network Connection Policy

Revised 8/20/2004

Committee Members:

Cheryl Albrecht - Associate Dean Univ. Library
Bill Bohmer - UCit NTS
Hal Carter - Department Head ECECS
Jim Downing - IT Security Officer UCit
William Fant - Associate Professor College of Pharmacy
Mark Faulkner - Executive Director UCit NTS
Daren Fowler - IT Deans Office CECH
Erma Fritsche - IT Manager Univ. Library
Richard Gass - Director A&S Physics
Karl Hart - IT College of Nursing
Jack Krebs - Director Engineering Computing Office
Perry Morgan - UCit OSA
Andrew Saunders - Director IT Pathology & Lab Medicine
Dan Wheeler - Associate Professor ECEH & EDU Foundation
David Will - IT Coordinator A&S Physics

University of Cincinnati Network Connection Policy

1.0 Introduction

The goal of this policy is to ensure a safe network-computing environment at the University of Cincinnati and achieve this as transparently as possible to the network user. Its design is to protect both information assets and members of the UC community from malicious programs and people. It will provide a reliable network environment in which end users have confidence and enhance the workflow and productivity of the University of Cincinnati community. (See Addendum A - Background.)

The University's General Policy on the Use of Information Technology establishes the framework for all information technology policies on campus. The Perimeter Firewall Policy covers the protection of the UC network from many Internet risks. This policy covers the protection from risks internal to the UC network and other external connection points such as remote access and wireless. The Information Technology Management Policy sets forth additional unit level responsibilities for the operation of computers connecting to the University of Cincinnati Network. UCit has the responsibility for the leadership, direction and enforcement of network and system security.

This policy applies to all members of the University of Cincinnati community and their visitors who have any device (computers, handheld devices, printers, game consoles, smart phones, etc.) connected to the UC network whether University owned or not. It also covers any kind of connection to the network, including direct-wired connections, modem connections, wireless connections, and Internet connections using virtual private network (VPN) software.
Policy implementation will occur in phases beginning with areas of the network outlined in section 3.x. The policy and the implementation plans will be reviewed during the phase-in and updated as necessary. The first review will take place no later than December 2004.

2.0 Policy

2.1 Overview

The major components of this policy are:

1. All devices connected to the UC network must be registered. Registration identifies the device, its location, and the people responsible for it.
2. All computers connected to the UC network must be maintained to minimize the risk that they could be used to compromise the security of the network. For personal computers this means that the operating system must be kept patched with the appropriate updates and that they must run anti-virus software with current virus signatures.
3. UCit will monitor the network for signs of malicious activity. The connections found to be responsible for suspected malicious activity will be switched to a restricted network that will enable the users to see that their connection has been restricted and which will enable them to access the resources that may assist in resolving the problem.

These policies apply to all devices connected to the UC network and must be followed by all users responsible for devices on the network. Implementation and enforcement of this policy will be diverse in different areas of the network. The following sections of this document explain the components of the policy in more detail and then a procedural companion document (Network Connection Procedures) will describe the implementation in each area of the network.

2.2 Registration

Devices may not be attached to the UC network until they are registered. The registration process will record the kind of device, location, and the people responsible for the device. The responsible people may include either the end user of the device or the area technical person responsible for the device or both. Registration of personal computers may require verification of the adherence to the security standards stated below.

A simple registration process will be available for providing access to University guests, both official guests on campus and student guests in residence halls and other student housing. The network may be configured so that guests have access only to those resources that are available to people connecting from outside the UC network.

Less intelligent computer devices, such as network printers, that cannot register via a web interface will need to go through a manual registration process.

Registration renewal occurs periodically to ensure that the information about devices connected to the network remains current.

2.3 Authentication
Registered devices will authenticate each time they connect to the network. This automated process is transparent to the network user because of the device specific information provided during the registration process.

2.4 Security Standards for Computers

All personal computers connected to the UC network (See Addendum A - Connection Methods) must have virus detection software installed and configured for automatic scanning for viruses and automatic checks for updated virus pattern files. UC provides site-licensed virus detection software that is available to all members of the UC community without cost. (Network Connection Procedures - See Addendum B.)

All computers connected to the UC network (See Addendum A - Connection Methods) must be maintainable in a state that will minimize their vulnerability to attack. This means that the operating system and network accessible programs must be patched with all available security-related updates. If possible, computers must be configured to automatically check for security updates and patches. (Network Connection Procedures - See Addendum C.)

2.5 Network Monitoring

UCit will monitor the UC network for signs of malicious or other inappropriate activity. This monitoring will include looking for use of ports associated with viruses or worms, attempts to make unauthorized access to other computers on the network, unusual patterns of heavy network activity, etc. When a device exhibits or is reported with any of these characteristics, UCit must investigate and take appropriate steps to protect the rest of the University network and its attached resources.

Devices identified as causing problems will be switched to a quarantine network. A web server on the quarantine network will inform the user of the problem and provide access to resources necessary to fix the problem. In cases of severe problems, a device may be removed entirely from access to the network. When it is necessary to quarantine or remove a device from the network, UCit will immediately notify both the registered end user and the technical person responsible for the device.

Note: UCit does not look at the contents of user files, whether they reside on an UCit-managed server, or on a personal system monitored for security problems.

3.0 Specifics for Different Locations or Kinds of Access

The implementation of this policy will vary. The sections below give the specific policies for the implementation of the policy in each area.

3.1 Student Housing

Beginning in the fall of 2004, a web registration process will be implemented that will include the installation of a smart-agent client on personal computers. This smart-agent client will verify that the operating system has been updated with the current patches and that the virus scanning is running with current virus definitions. Only if the system meets the requirements of the policy will it be allowed on the system. The smart-agent will verify that the system is up-to-date each time the personal computer is connected to the network. (Network Connection Procedures - See Addendum D.)
Students will also be able to register devices which are not personal computers and which cannot run
the smart-agent.

Registration will occur at the beginning of each school year and on rare occurrences more often.

**Addendum A**

**Background**

Failure to apply appropriate security patches to desktop and server vulnerabilities is the single largest
risk to enterprise data and availability of its resources and infrastructure. The majority of enterprise
security breaches result from viral or worm-based attacks. Developers of these attacks are exploiting
vulnerabilities at an increasing rate and support personnel must react quickly to apply system patches
before major disruptions occur. In the past, the University’s network security perimeter design and
architecture provided the time to respond to and mitigate the number of infections within the
University’s network. However, attacks are becoming increasingly sophisticated using common
application communication ports from the Internet, therefore fighting infection and propagation has
become more difficult.

Vulnerable computer systems may result in the following consequences for the enterprise:

- Higher costs associated with infection or security breach cleanup
- Direct loss of revenue from system outages and declining productivity
- Indirect financial loss due to loss of reputation and/or customer confidence
- Legal liabilities from breach of sensitive records
- Loss or corruption of business data
- System downtime, inability to conduct business
- Theft of information assets

Increases in non-traditional teaching methods and the mobility of faculty and students have made
security increasingly important. Rising frequency of computer abuse incidents involving network-
attached devices significantly increases the probability of major disruptions to the University’s internal
computer systems. Any element of the University network or internal computer systems that has
uncontrolled or unsecured paths must have sufficient security measures in place to protect the entire
University infrastructure.

**Connection Methods**

University of Cincinnati users may connect computers to the campus network at appropriate
connectivity points: voice/data jacks or through an approved wire network access point.

The policy of the University of Cincinnati is that only authorized Information Technology staff may
install, manage, or change the network infrastructure. Unauthorized changes to the network can
seriously compromise the reliability, performance, security and availability of the network and its
services. In addition, illegal wiring may be in violation of FCC regulations, and fire or building codes,
which may create a public safety hazard.
Extensions or modifications to the network or installation of hardware devices including, but not limited to, bridges, switches, wireless access points, or hubs without written permission from UCit is prohibited to ensure the integrity and availability of the entire University network.

Network Connection Procedures
(Companion Document to Network Connection Policy)

The Network Connection Procedures is a companion document to the University of Cincinnati Network Connection Policy. This section is an operational document subject to modification as technology changes.

Addendum B

UCit anti-virus software
Computer Viruses - Tutorial

General Tips for Overall Computer Protection
formerly at http://www.ucit.uc.edu/computers/software/GeneralTips.asp

Addendum C

Microsoft Windows Operating Systems:

Automatic Update: for computers unable to use SUS
Windows XP Pro
Windows 2000
Windows ME
Windows 98

Manual Windows Update: for computers unable to use Automatic Update

Open Internet Explorer (IE) as your browser. Point your browser at windowsupdate.microsoft.com and follow the online instructions.

UCit recommends utilizing Windows XP Pro on computers connecting to the UC network.

Macintosh OSX (10.x):

Using the Macintosh OSX automatic Software Update feature from System Preferences, you can request updates (Internet) at any time or schedule when Mac OS X checks for updates (daily/weekly/monthly).

Online directions are available.

Run Update Now and then configure Schedule and Update (daily).

UCit recommends utilizing Mac OSX (10.x) on computers connecting to the UC network.
**UNIX environments:**

Solaris Security:  
Linux Security:  
[http://www.linux-sec.net](http://www.linux-sec.net)

**Addendum D - Student Housing Procedures**

Last fall, outbreaks of viruses coincided with the arrival of new and returning students. Most of the students' Windows computers did not have current security patches from Microsoft. Most either had no virus protection software or had software that was out of date and unable to detect the viruses that were circulating.

The University has automated the residential hall information technology sign-on process to secure the integrity and availability of the university's network. Each computer that is using a University of Cincinnati student housing network connection will be required to go through an automated registration and security screening process.

Next fall, 2004-2005 school year, network security measures will be in place to heighten personal computer security, boost network reliability, and amplify UCit capacity to diagnose computers with viral infections or other malicious activity. The solution will require all University of Cincinnati housing students to sign-on the UC Network.

As student housing computers connect to the network security screening system a smart-agent will determine if each is safe and verify if the anti-virus pattern file and operating system update are current.

If both are current, the system gives the user permission to use the network. If not, the system quarantines the user to the appropriate web sites to obtain the necessary updates for anti-virus software and/or operating system. The user must then install the appropriate update before permitted to use the network.

The system automatically scans the UC housing student network for infected or vulnerable systems.

This automation should improve the turnaround time for students to register and connect to the campus network for services. This will keep virus infections to a minimum and at the same time enforce updates and patches to prevent future problems.

**Registration and Authentication Process:**

Depending on how up-to-date your Windows operating system is, this procedure can take from a few minutes to an hour. To facilitate the process and save time, download and install the latest Windows Operating System Service Packs and Critical Updates before you start the following procedure.

The new process will consist of three steps.
Log-on to the University web page, accept the University of Cincinnati General IT Use policies and download and install the smart-agent client onto your personal computer.

The smart-agent then scans your machine to check for the existence of the University's approved virus protection program. If this software needs installed on your personal computer, you will be given access to download and install it. As a student of the University of Cincinnati, the software is provided at no cost to you (See Addendum B.) After installing the anti-virus program, you will be asked to restart your machine.

At this point, your machine will authenticate and be scanned again to make sure all operating system service packs are up-to-date and all critical security updates are installed. If not, you will be redirected to a website to download necessary service packs and critical updates.

If your computer passes the scan, you will be given access to the network.