

Responsibilities for Computing Devices Connected to the University of Virginia Network

Policy Guide

UVa Information Technology and Communication Department

UVa Health Systems Computing Services Department

May 11, 2006

Table of Contents

1.0 INTRODUCTION.....	ERROR! BOOKMARK NOT DEFINED.
2.0 ROLE OF DEANS, DEPARTMENT HEADS AND PRINCIPAL INVESTIGATORS	ERROR! BOOKMARK NOT DEFINED.
3.0 ROLE OF ITC AND HS/CS	ERROR! BOOKMARK NOT DEFINED.
4.0 OPTIONS FOR SECURITY COMPUTER DEVICES	ERROR! BOOKMARK NOT DEFINED.
4.1 SINGLE-USER PCs AND MACS	ERROR! BOOKMARK NOT DEFINED.
<i>4.1.4 Needed Actions for Securing Single PCs and Macs</i>	<i>Error! Bookmark not defined.</i>
<i>4.1.2 Time Commitment for Securing Single-user PCs and Macs</i>	<i>Error! Bookmark not defined.</i>
<i>4.1.3 Technical Skills for Security Single-user PCs and Macs</i>	<i>Error! Bookmark not defined.</i>
<i>4.1.4 Possible Strategies for Securing Single-user PCs and Macs</i>	<i>Error! Bookmark not defined.</i>
4.2 SERVERS.....	ERROR! BOOKMARK NOT DEFINED.
<i>4.2.1 Needed Actions for Securing Servers</i>	<i>Error! Bookmark not defined.</i>
<i>4.2.2 Time Commitment for Securing Servers.....</i>	<i>Error! Bookmark not defined.</i>
<i>4.2.3 Technical Skills for Securing Servers</i>	<i>Error! Bookmark not defined.</i>
<i>4.2.4 Possible Strategies for Securing Servers.....</i>	<i>Error! Bookmark not defined.</i>
APPENDIX I: RESPONSIBILITIES FOR COMPUTING DEVICES CONNECTED TO THE UNIVERSITY OF VIRGINIA NETWORK POLICY	8
APPENDIX II: PROCEDURE FOR BLOCKING A COMPUTING DEVICE'S ACCESS TO THE UVA NETWORK.....	11
APPENDIX III: FREQUENTLY ASKED QUESTIONS	12
APPENDIX IV: ITC AND HS/CS SERVICES THAT CAN BE LEVERAGED TO SECURE DEVICES.....	16
APPENDIX V: TRAINING SOURCES	20
APPENDIX VI: HIRING CRITERIA	22

1.0 INTRODUCTION

Benefits of the Internet are being realized today in all facets of our lives, and use is continuing to grow at a rapid pace. Accompanying that welcomed growth, however, are increasing opportunities and temptations for misuse of the Internet resource, and these are being taken advantage of in a big way. Computer attacks are increasing and doing more harm than ever before. In 2005, the damaging effects of malware had a total cost of \$14.2 billion worldwide.

Universities are unfortunately favorite targets of computer attackers. Critical University computing resources, such as research, patient, and student data, are at risk, and University computers (both single user workstations and servers) are being taken over by cybercriminals and used as platforms to attack other universities, corporations, government agencies and other entities. The consequences of not addressing this problem can be loss of staff productivity, loss of assets, a tarnished reputation, and litigation.

While it may never be possible to intercept all attempts of attacks - new forms of attack are being devised every day -- there are steps that can be taken at the University of Virginia to significantly reduce vulnerabilities. Because an attacker can seize a vulnerable device and use it to launch an attack on others, it is important that everyone owning or overseeing the use of a computing device connected to the University's network assume responsibility for securing that device. We can only be as strong as our weakest link.

The University has put a policy (see [Appendix I](#)¹⁸) in place that defines requirements for device owners and overseers to close security gaps. The policy stipulates that when University network resources and privileges are threatened by an improperly maintained computing device, the Information Technology and Communication (ITC) Department and Health Systems Computing Services (HS/CS) may act on behalf of the University to remove the threat by working with the device owner or overseer to quickly close security holes. In an emergency or when collaboration fails, the device may be disconnected from the network until security vulnerabilities are addressed.

ITC and HS/CS have developed this policy guide and a [web site](#)²⁴ of helpful information and guidance for addressing this policy. They also offer services device owners and overseers may find valuable.

2.0 ROLE OF DEANS, DEPARTMENT HEADS AND PRINCIPAL INVESTIGATORS

Because of their leadership positions and control over resources, deans, department heads and Principal Investigators (PIs) can play a critical role in the successful implementation of this policy. Specifically, they can use their influence to:

- Make computer security a staffing and funding priority. Additionally, PIs can specify the cost associated with security as a direct cost in grant proposals.
- Change attitudes and behaviors within the units they lead by communicating the importance of addressing security vulnerabilities and by requiring all staff

members to be responsible and accountable for the security of their network-connected devices.

- Ensure units acknowledge that administering servers takes specialized skills and have only qualified people do this work.
- Ensure device owners and overseers in their units take swift action should a security breach occur and seek help from ITC or HS/CS if needed.

3.0 ROLE OF ITC AND HS/CS

ITC and HS/CS are responsible for closing security gaps on all devices they own themselves and manage for others through service contracts. These departments also employ intrusion detection systems at the outside perimeter of the University network and special purpose firewalls in various locations that help reduce some threatening network traffic. In addition, ITC and HS/CS fill a pivotal role in providing services that aid other university departments in carrying out their responsibilities for the policy. These services are listed below and described in greater deal in [Appendix IV](#)²¹. ITC and HS/CS Services That Can Be Leveraged Secure Devices:

- A [web site](#)²⁴ containing current information on security best practices and on known vulnerabilities and ways to eliminate them is maintained.
- Alerts of dangerous new computer viruses and instructions for protecting devices from them are sent to appropriate mail lists and posted on the University and ITC web sites as they occur.
- Various contract services are available for shared central hardware/software use and for installation and/or ongoing support of department-owned computers.
- Secure standard software configurations are available through ITC's Desktop Computing Initiative and Premium Desktop offerings and through HS/CS' Desktop Standard.
- Site licenses for various security tools are provided.
- Education and training opportunities that incorporate security topics into broader curricula are offered. In addition, ITC and HS/CS operate programs that help departmental computing support staff gain skills and knowledge necessary to provide effective technical support for their departments.
- ITC offers a consulting service that assists departments with the development and implementation of technology plans, including requirements for technical skills and staffing.
- ITC and HS/CS serve as points of contact and sources of advice when a department's computer is attacked.

4.0 OPTIONS FOR SECURING COMPUTER DEVICES

Strategies and staffing currently employed for addressing security may be adequate in some departments and programs; however, new approaches are likely to be needed in many areas. Security needs and strategies for addressing them can vary widely depending

upon the number of computing devices, the device types, the purposes for which those devices are used, the technical skills levels of existing staff, and other factors. While there is no single solution that can be recommended, there are basic rules of thumb that can be used in determining an appropriate course of action. This section provides guidance to deans, department heads, and PIs on the basic ongoing security activities required, rules of thumb regarding time and skill needs, and options available for acquiring these services.

In most departments a combination of single-user PCs and Macs computers and multi-user servers are deployed. While there are a few similarities in the actions required to secure single-user computers and multi-user servers, the degrees of complexity are quite different. For this reason guidance is provided on each separately.

I. 4.1 Single-user PCs and Macs

4.1.1 Needed Actions for Securing Single-user PCs and Macs

Keeping single user PC and Mac machines secure requires that the following set of actions be performed on those devices on an ongoing basis. (The complete list of these settings with explanatory details can be found at [Quick Tips for Personal Computers](#)²⁵.)

- a. [Use strong password protection](#)²⁶
- b. [Use a password protected screensaver](#)²⁷
- c. [Keep files from unknown sources off the device](#)²⁸
- d. [Backup files](#)²⁹
- e. [Use up to date anti-virus software](#)³⁰
- f. [Keep the device's operating system updated](#)³¹
- g. [Keep the device's application software updated](#)³²
- h. [Turn off or delete unneeded software features](#)³³
- i. [Limit access to the device](#)³⁴
- j. [Enable your operating system firewall](#)³⁵
- k. [Regularly request security vulnerability scan report](#)³⁶

II. Important note to Health System employees: If your device is managed by Health Systems Computing Services, actions *d* through *i* are handled by HS/CS staff members. Actions *a*, *b* and *c* are the responsibility of individual device owners.

III. 4.1.2 Time Commitment for Securing Single-user PCs and Macs

The time required to keep a PC or Mac secure varies widely depending upon how the device is used, the technical skills of the person doing the work, the level of vulnerabilities and hacker activity at a given point of time, and other factors. A rule of thumb, however, is that it will take between 30 to 90 minutes per device per month to accomplish needed actions. An economy of scale does apply. The amount of time required per device goes down as the number of similarly configured devices managed by a single person goes up. Desktop workstations can be centrally managed given the appropriate level of skill of the system administrator. Factors that influence the decision to centrally manage computers include the following: number of computers, sensitivity of

data, and propriety for the user culture. Note that the time commitment should be less for HS/CS customers using the HS/CS Desktop Management service.

IV. 4.1.3 Technical Skills for Securing Single-user PCs and Macs

The skills of a technical professional are not necessarily required to carry out the actions described for single-user PCs and Macs; however, the device user does need to have more than a basic understanding of the operating system and other software running on the device. For example, a person performing the actions must be comfortable with the technical jargon often used by software manufacturers to describe security vulnerabilities and software updates to address them. As important as the skill level, the person must also have the time and commitment to accomplish needed actions.

V. 4.1.4 Possible Strategies for Securing Single-user PCs and Macs

It is important to understand that securing single-user PCs and Macs is an ongoing process. New vulnerabilities are constantly being identified, and it is important to stay vigilant and take appropriate actions as needed. Possible strategies that can be taken to install secure systems in the first place and to keep them secure after installation are described briefly below. Additional information may be found in:

[Appendix IV](#)²¹ - ITC and HS/CS Services That Can Be Leveraged to Secure Devices

[Appendix V](#)²² - Training Sources

[Appendix VI](#)²³ - Hiring Criteria

Strategies for installing secure single-user devices:

Select standard Desktop Computing Initiative (DCI) devices - The DCI Program offers acquisition options and installation services for standard models of single-user PC and Mac computers. DCI computers are delivered configured to work in the U.Va. environment and are pre-loaded with a standard suite of software and basic applications. Security vulnerabilities known at the time a DCI device is acquired are addressed before delivery; however, department and program heads need to employ strategies to keep the device secure after installation.

Use ITC's Premium Desktop configuration for Windows-based devices - For those with computer needs not met by the standard models available through the DCI Program, ITC offers customizable, modular, and secure Windows XP desktop configurations with a standard suite of software and basic applications. As with the DCI devices, strategies to keep Premium Desktop configurations secure after they are installed are also needed.

Use HS/CS Desktop Standard - HS/CS administrative customers should follow HS/CS desktop standard for hardware and software.

Strategies for maintaining secure single-user PC and Mac devices:

HS/CS Desktop Management System - Hospital departments may use the HS/CS systems management system, which provides many benefits in terms of timely and consistent desktop support. This service is mandated for all IHMS users.

Train existing staff person(s) - ITC offers training for U.Va. personnel who have the time, ability and interest to learn basic computer skills, including those needed to secure PCs and Macs. See Appendix VI for training sources

Share skilled person with another department - Departments/programs with few PCs and Macs may be able to work out an arrangement whereby a skilled person is shared across multiple departments/programs.

Contract for maintenance services with an outside firm - There are firms in the Charlottesville area that offer full maintenance services for PCs and Macs, including keeping devices secure. Quality of service varies, so it is important to check references before signing a contract.

VI. 4.2 Servers

VII. 4.2.1 Needed Actions for Securing Servers

All actions required to keep single-user PCs and Macs secure also apply to servers. The work is much more complex, however, because multiple users could be affected by every action, servers often utilize more software (and can, therefore, have more vulnerabilities) than single-user devices, and other factors. There are also additional actions needed, which vary widely depending upon the function of the server. There are, for example, special considerations for servers used to host websites, mail services, and other functions. These special considerations are too detailed to mention here, but are explained at the [Community Security Baseline](#)³⁷.

VIII. 4.2.2 Time Commitment for Securing Servers

The time required to keep a server secure varies widely depending upon how the device is used, the number of people using it, the age of the software on it, the technical skills of the person doing the work, the level of vulnerabilities and hacker activity at any given point of time, and other factors. A rule of thumb, however, is that it will take 16 or more hours per server per month to accomplish the needed actions. An economy of scale does apply. The amount of time needed per server goes down as the number of similarly configured servers managed by a single person goes up.

IX. 4.2.3 Technical Skills for Securing Servers

A person who is well trained and experienced in computer system administration is needed to accomplish the work associated with securing servers. Indeed, assigning someone who does not have the necessary knowledge and skills can do more harm than good. In addition to appropriate technical skills, the person must also have the time and commitment to accomplish needed actions.

X. 4.2.4 Possible Strategies for Securing Servers

As with single-user devices, securing servers is an ongoing process. New vulnerabilities are constantly being identified, and it is important to stay vigilant and take appropriate actions as needed. Possible strategies that can be taken to install secure servers in the first place and to keep them secure after installation are described briefly below. Additional information may be found in:

[Appendix IV](#)²¹ - ITC and HS/CS Services That Can Be Leveraged to Secure Devices

[Appendix V](#)²² - Training Sources

[Appendix VI](#)²³ - Hiring Criteria

Strategies for installing secure servers:

Contract for use of centralized shared servers instead of purchasing servers - As an alternative to purchasing a departmental server, departments make take advantage of [ITC Premium Server](#)³⁸ service, which provides hardware, software, and file space. ITC staff time to administer and maintain the server, including addressing security vulnerabilities, is included in the contract. HS/CS offers a similar service to hospital departments with its file and print (Super) servers.

Contract with ITC or HS/CS to install servers - ITC and HS/CS staff are available to install and make secure servers purchased by departments they support. It is critical that strategies to keep the servers secure on an ongoing basis also be employed. See Appendix IV for more information.

Strategies for maintaining secure servers:

Contract with ITC or HS/CS to maintain the servers - ITC provides operating systems support, file system backups, and operational support on an annual fee basis for Unix, Linux, and Windows-based servers. Additionally, services are available at an hourly rate installation of operating system upgrades and other services that can help maintain the security of servers. HS/CS offers similar services for servers owned by departments in the hospital. See Appendix IV for more information.

Share skilled system administrator with another department - If the number and complexity of the servers is low, departments may find it feasible to share a skilled system administrator.

Hire a system administrator - Recommended hiring criteria is provided in Appendix VI for departments wishing to hire a permanent, full-time system administrator for their departments.

Train existing, technical savvy staff person(s) - Some firms in Charlottesville and Piedmont Virginia Community College offer training on system administration, and many good certification programs are available from national security organizations. See Appendix V for training sources.

Contract with an outside firm for maintenance services - There are firms in the Charlottesville are that offer maintenance services for servers, including keeping these devices secure. Quality of service varies, so it is important to check references before signing a contract.

Appendix I: Responsibilities for Computing Devices Connected to the University of Virginia Network Policy

Purpose

The purpose of this policy is to clearly define requirements for owners and overseers of University of Virginia network-connected devices to close security gaps. It also describes loss of network access for non-compliance, as well as an exception process.

Policy Statement

Those responsible for devices connected to the University of Virginia network must ensure that key security vulnerabilities are eliminated from these devices.

Background

Although the rapid growth of legitimate new uses of the Internet is quite welcomed, this growth has at the same time increased the opportunities and temptations for misuse of the Internet resource. Security breaches at highly visible computing sites have become commonplace today, and universities are favorite targets for attacks. Critical university computing resources, such as research, patient care, and student data, are at risk, and university computing devices are being commandeered by cybercriminals to launch attacks on corporations and other entities outside the university.

While it is not possible to anticipate and intercept all attacks -- cybercriminals are continuously devising new ways to wreak havoc -- there are specific steps that can be taken to significantly reduce vulnerability. These steps are effective, however, only if they are taken for all devices on the University of Virginia's network. The saying that "we are only as strong as our weakest link" most definitely applies in this case.

Key security gaps that need to be closed may vary depending upon the type of device. Some examples follow.

- a. All device owners should ensure passwords used on their devices are not easily guessable by attackers.
- b. Owners of personal computers should install and run anti-virus software on these devices and apply updates from the software vendor as they become available.
- c. Owners of personal computers and servers should apply security-related updates to the operating system running on their devices as these updates become available from operating system vendors. Examples of a few operating systems found at UVa are Windows 2000, Windows NT, and Red Hat Linux.
- d. Owners of UNIX and Linux servers should switch off unneeded services to eliminate the risk of these being exploited.

It is important to note that the above are examples only and do not represent a complete list of known security vulnerabilities.

Vulnerabilities that are considered "key" will change over time as new threats and risks surface. Information Technology and Communication (ITC) and Health Systems Computing Services (HS/CS) maintain a current list of key vulnerabilities and steps required to close the vulnerabilities. Device owners/overseers are responsible for staying apprised of changes to this list and acting promptly to address any new security gaps defined.

ITC and HS/CS wish to work in partnership with owners and overseers in fulfilling the responsibilities outlined in this policy. A frequently asked questions document is available to answer questions about the policy and provide guidance on obtaining advice or help.

Scope

This policy applies to anyone in the university community owning or overseeing the use of a computing device of any type connected to the University of Virginia network, including but not limited to:

- a. ITC or HS/CS, if the devices are under ongoing support contracts with these organizations;
- b. Faculty, staff, students and other individuals who have devices connected to UVa's network, even if those devices were acquired personally, i.e. not with university or grant funds;
- c. UVa department heads, even in cases where vendor owned and/or managed equipment is housed in departments;
- d. Research project Principal Investigators, if their projects use devices connected to UVa's network.

If no one claims responsibility for a device, the UVa department head for the department in which the device resides will be presumed to be responsible by default.

This policy is especially focused on individuals responsible (as defined above) for devices that serve more than one user. It should be noted, however, that the required actions outlined in this policy are appropriate and must be undertaken by those responsible for single-user devices as well. When devices are used for university business, compliance will be verified by the University's Audit Department during routine audits.

Enforcement

In cases where University network resources and privileges are threatened by improperly maintained computing devices, ITC and HS/CS may act on behalf of the University to

eliminate the threat by working with the relevant device owner or overseer to quickly close security holes. In circumstances where these collaborative efforts fail or there is an urgent situation requiring immediate action and leaving no time for collaboration, the device may be disconnected from the network by ITC or HS/CS (which department depends upon the location of the device). Reference the procedure for revoking network access of connected equipment for more specific information.

Exceptions

Requests for exceptions to this policy should be made in writing (hard copy or email) to the VP/CIO. An exception may be granted if it is clear that the benefits to the University of the vulnerable device far outweigh the risks, as judged by the VP/CIO.

Source of Policy: Written by the Office of the VP/CIO and approved by the University of Virginia President's Cabinet

Effective Date/Revised Date: July 1, 2001

Review Frequency: Yearly by the Office of the VP/CIO

Appendix II: Procedure for Blocking a Computing Device's Access to the UVa Network

In cases where University network resources and privileges are threatened by improperly maintained computing devices, Information Technology and Communication (ITC) and Health Systems Computing Services (HS/CS) may act on behalf of the University to eliminate the threat by working with the relevant device owner or overseer to quickly close security holes. In circumstances when these collaborative efforts fail or there is an urgent situation requiring immediate action and leaving no time for collaboration, the procedure that follows will be used. The procedure applies to any computing device connected to the University of Virginia network.

1. Designated ITC and HS/CS system administrators may block network access for a device to safeguard University resources and protect University privileges, as explained in the University-wide "Responsibilities for Computing Devices Connected to the University of Virginia Network Policy." Which of the two IT organizations blocks access is dictated by the part of the network to which the offending device is connected.
2. Such blocks will persist until the device problems have been resolved to the satisfaction of the Vice President and Chief Information Officer (VP/CIO) of the University or the Health Systems Chief Information Officer, as appropriate.

Appendix III: Frequently Asked Questions

Enforcing the Policy

1. Who determines when to take action?

Information Technology and Communication (ITC) and Health System Computing Services (HS/CS) are neither investigative nor disciplinary entities in their primary responsibilities. However, in cases where University network resources and privileges are threatened by improperly maintained computing devices, these departments must take appropriate steps. Before taking action, however, ITC and HS/CS will attempt to resolve the problem in collaboration with the device owner or overseer, unless the situation is so urgent that immediate action is required and there is no time for collaboration. In the latter case, ITC and HS/CS will inform the owner or overseer as soon as practical and provide advice as needed to resolve the problem.

2. How will ITC and HS/CS identify vulnerabilities?

Security vulnerabilities on a given device are usually discovered as the result of an investigation of a problem reported from someone within or outside the university who is being attacked from that device or during an audit conducted by the University's Audit Department or other auditing organizations. Also, ITC offers a proactive network scanning service that can report vulnerabilities to the person requesting the scan before the security holes actually cause problems. As already stated, ITC and HS/CS will make an attempt to resolve the problem in collaboration with the device owner or overseer before taking action, unless the situation is so urgent that immediate action is required.

3. If somebody's PC propagates a virus mailing, will that PC be unplugged?

The policy will not be used to punish anyone. Its purpose is to help protect the university's networked environment as a whole. Before taking action, an attempt will be made to resolve the problem in collaboration with the device owner or overseer. The availability of PC virus software makes remedies for mail viruses usually simple to apply. For this reason it seems highly likely that, in the event of a virus mailing problem, collaboration with the device owner or overseer will result in quick and satisfactory resolution.

4. Will an operating system not formally supported by ITC or HS/CS be deemed unacceptable, if someone in ITC or HS/CS believes it not to be secure?

It is not the intent of the policy to deem operating systems as a whole, either supported or not, to be unacceptable. Key vulnerabilities will be listed on a website maintained by ITC and HS/CS and most will be drawn from a consensus list developed by the highly

regarded SANS Institute in collaboration with the Department of Justice and the FBI. The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions for challenges they face. Suggested remedies take the form of applying software patches, changing configuration settings, changing passwords, and the like. None of the remedies suggest replacing one operating system with a totally different one. ITC and HS/CS will not, however, be able to provide the same level of assistance and advice to unsupported environments as it does to supported ones.

Addressing the Policy

5. Who will provide information (and in what form?) to deal with such vulnerabilities? Who determines what vulnerabilities are key?

As mentioned in under question 5, ITC and HS/CS will maintain a website describing critical vulnerabilities and remedies relevant to our environment. The source of some of this information will be the SANS Institute consensus list of key vulnerabilities.

6. What are some examples of key vulnerabilities?

Key security gaps that need to be closed may vary depending upon the type of device. Some examples follow.

- a. All device owners should ensure passwords used on their devices are not easily guessable by attackers.
- b. Owners of personal computers should install and run anti-virus software on these devices and apply updates from the software vendor as they become available.
- c. Owners of personal computers and servers should apply security-related updates to the operating system running on their devices as these updates become available from operating system vendors. Examples of a few operating systems found at UVa are Windows 2000, Windows NT, and Red Hat Linux.
- d. Owners of UNIX and Linux servers should switch off unneeded services to eliminate the risk of these being exploited.

It is important to note that the above are examples only and do not represent a complete list of known security vulnerabilities.

Vulnerabilities that are considered "key" will change over time as new threats and risks surface.

7. What, if any, assistance can device owners expect, aside from a list of vulnerabilities?

The website will provide explanations of remedies as well as vulnerabilities. ITC and HS/CS also offer installation and maintenance services for department-owned computing

devices, consulting services, and help desks for assistance with problems. Additionally, presentations on security topics have been and will continue to be given at LSP meetings, and work on other security awareness education and training strategies is ongoing.

8. What are the responsibilities of device owners who contract with ITC or HS/CS to administer their machines?

The policy states compliance is the responsibility of ITC or HS/CS if the devices are under ongoing support contracts with these organizations. Users are responsible for approving and allowing necessary security upgrades to be made rapidly by ITC or HS/CS. Users are responsible for not circumventing security configurations installed by ITC or HS/CS.

9. Does the University provide adequate resources to the departments and schools to administer and operate their technical infrastructure?

Additional resources are always welcomed, but there are at least three things departments and schools could do to improve their ability to administer and operate their technical infrastructure:

- a. ITC and HS/CS offer installation and maintenance contracts for computing devices in departments. Taking advantage of these services could be less expensive overall for departments and schools than installing and maintaining the devices on their own.
- b. Researchers should always include the cost of maintaining and operating new equipment that is funded by grants. This could take the form of purchasing support from ITC or HS/CS or hiring a skilled system administrator.
- c. ITC offers a free scanning tool service that will automatically detect and report to the requestor security vulnerabilities on computing devices. Departments and schools could request that scans be run on a regular basis.

The Concern

10. Why is this policy needed?

Although malicious intent is possible, the lack of attention to security vulnerabilities is the target of this policy. Inattention to security vulnerabilities is a realistic concern as evidenced by a number of high profile attacks on computing environments of universities and other organizations.

Security breaches at highly visible computing sites have become commonplace today, and universities are favorite targets for attacks. Critical university computing resources, such as research, patient care, and student data, are at risk, and university computing devices are being commandeered by cybercriminals to launch attacks on corporations and other entities outside the university.

While it is not possible to anticipate and intercept all attacks -- cybercriminals are

continuously devising new ways to wreak havoc -- there are specific steps that can be taken to significantly reduce vulnerability. These steps are effective, however, only if they are taken for all devices on the University of Virginia's network. The saying that "we are only as strong as our weakest link" most definitely applies in this case.

Appendix IV: ITC and HS/CS Services that Can Be Leveraged to Secure Devices

Single-user PC and Mac Systems Services

DCI Program

The Desktop Computing Initiative is a voluntary, university-wide program designed to curb the total cost of owning computers and to increase the efficiency and effectiveness of support for personal computing at the University.

Cost for the Dell DCI Standard Desktop with Windows 98: \$1,179. Other models and prices available.

Details at: <http://www.itc.virginia.edu/dci/dci-general/>

Premium Desktop Service

The Premium Desktop Service is a customizable, modular, and secure Windows NT 4.0 desktop with a standard suite of software and basic applications.

Cost: \$5 - \$100, one-time software licenses (depending on software selected)

Details at: <http://premium.itc.virginia.edu/desktop/>

Site-licensed Software Related To Security

ITC's Software Central site contains software licensed for use by faculty, staff, and students. There is no charge to download and install this software. Security related software includes Norton Anti-virus (virus protection), SecureCRT (secure Telnet connections), and (Spring 2001) SecureFX (secure FTP file transfer).

Details at: <http://www.itc.virginia.edu/desktop/central/>

HS/CS Desktop Management

HS/CS employs Microsoft System Management Server (SMS) to deliver more timely and consistent desktop support. Capabilities include automated inventory, software and anti-virus distribution, and remote control by Help Desk staff. Service is free to hospital departments.

Details at: <http://www.mcc.virginia.edu/mcc/news/deskmng.htm>

Server Services

Premium Server Service

The Premium Server Service offers space on an NT file server to departments. The Service provides departments with shared workspace and provides individuals with their own secure directories.

Cost: \$125/yr for each Gb of storage

Details at: <http://premium.itc.virginia.edu/server/>

Micro Systems Department Server Support

The ITC Departmental Micro Systems Support program provides operating system support, file system backups and operational support for department-owned Microsoft Windows NT 4 and Windows 2000 servers.

Cost: \$2,050/yr for systems up to 50Gb storage, with backup

Details at: http://www.itc.virginia.edu/microsys/mcs_support.html

Departmental Unix Systems Support Program

The ITC Departmental Unix Systems Support program provides operating systems support, file system backups, and operational support for department-owned Sun, IBM RS/6000, SGI, and Intel-Linux Red Hat 6.2 servers.

Cost: \$1,500/yr for systems up to 50Gb storage, with backup. Additional systems are \$1,000 with backup.

Details at: <http://www.itc.virginia.edu/unixsys/support.html>

HS/CS File and Print (“Super Server”) Services

HS/CS offers centrally maintained server services for hospital departments. For details, contact the HS/CS Help Desk at 924-5334.

Departmental Security Services for All Hardware Platforms

The following additional services and information services provided by ITC and HS/CS are relevant to all hardware platforms:

Security Best Practices

ITC maintains a web site of current information on security best practices and known vulnerabilities. The site can be found at:

<http://www.itc.virginia.edu/security/vulnerabilities.html>

Virus Alerts

HS/CS and ITC staffs jointly monitor virus activity and post virus alerts on the University and ITC home pages and selected mail lists. ITC's Virus Hot Topics page provides a comprehensive review:

<http://www.itc.virginia.edu/desktop/security/virushottopics.html>

Information about HS/CS virus protection can be found at:

<http://www.mcc.virginia.edu/mcc/helpdesk/faq.html#virus>

Points of Contact for Computer Security Problems

Faculty, staff, and students can report computer security problems by calling the ITC Help Desk (924-3731) or sending e-mail to abuse@Virginia.edu or consult@Virginia.edu. Health system employees can contact the HS/CS Help Desk (924-5334) or send e-mail to helpdesk@hscmail.mcc.Virginia.edu.

Departmental Planning and Outreach

ITC's Departmental Computing Support group consults with departments to assess technology needs, help develop a technology plan, and assist with the implementation of the plan. Information can be found at:

<http://www.itc.virginia.edu/dcs/dpo/>

Local Support Partner (LSP) and Local Support Associate (LSA) Programs

These two programs help departmental computing support staff gain skills and knowledge necessary to provide effective technical support for their departments.

The LSP Program is an alliance between ITC and computing professionals serving departments throughout the University and is part of ITC's Departmental Computing Support Program. Through certification-directed training, high-level access to ITC resources and services, and regular liaison activities, Local Support Partners are provided with important tools to help them be more successful in their departmental computing roles. Details can be found at:

<http://www.itc.virginia.edu/dcs/lsp/>

The LSA Program is designed to provide front-line technical support staff with knowledge of the University of Virginia's computing environment, so they can provide effective computing support within their department. Details are available at:

http://www.itc.virginia.edu/dcs/lsp/css/lsa_program.htm

HS/CS Client Services Meeting

HS/CS hosts periodic meetings to exchange information with department computing support staff. For more information, contact Richard Shelley, HS/CS client services manager, at 924-8292 or ras2m@virginia.edu.

UVa Security Scanning

ITC provides a free service to scan computers for known security vulnerabilities and produce a report for the user or department. The service uses Internet Security system's Internet Scanner, which locates vulnerabilities like an intruder would - by examining a network's devices, services, and interrelationships. Internet Scanner provides detailed information about the vulnerabilities found, including the vulnerable host, a description of the vulnerability, and the steps to take to eliminate the vulnerability. Information on requesting a scan can be found at: <http://www.itc.Virginia.EDU/netsys/security/iss/issdoc.html>

Information on Hardware and Software Firewalls

Under certain circumstances, hardware firewalls can be used to increase security of critical servers. Information about the use of hardware firewalls at the University can be found at:

<http://www.itc.virginia.edu/netsys/security/firewalls/hardwarefirewall.html>

Several commercial software firewalls are available to increase security on individual computers. However, their ease of use and potential benefits vary. An ITC review of some of these products can be found at:

<http://www.itc.virginia.edu/netsys/security/firewalls/firewalls.html>

Appendix V: Training Sources

Training Sources for Non-technical Individual Users

ITC Training offers a variety of workshops and short courses designed to enhance individual proficiency. Where appropriate, security issues are addressed.

Computing Survival Skills

Developed in conjunction with the Local Support Associate program, this comprehensive training program is designed to teach staff members the basic computing skills and knowledge necessary to provide efficient and effective technical computing support within their departments. One module is devoted to security issues. For details, see: <http://www.itc.virginia.edu/dcs/lsp/css/home.html>

Office Technology Conferences

This annual conference, which provides introductory sessions on current and emerging computing technologies, is open to all office professionals, including faculty, managers, supervisors and administrative staff, as well as technical and computer professionals. Typically one session focuses on computer security. Information can be found at: <http://www.itc.virginia.edu/training/conferences/>

LSP Conferences

One of the benefits of the LSP program is participation in the semi-annual conferences. Security policy and technology are often topics at these conferences. Information about the program is available at: <http://www.itc.virginia.edu/dcs/lsp/>

Computer Workshops

ITC-Training offers the University community a variety of software training workshops, designed to promote the effective use of a variety of popular software products and operating systems. Security topics are presented in the context of the particular software. Details and current course list can be found at: <http://www.itc.virginia.edu/training/wkshp.html>

ITC Broadcasting

ITC Broadcasting provides free computer training for all University of Virginia faculty, staff and students through The Academic Access Channel and a videotape/CD-ROM checkout library. Training materials cover introductory and technical topics. For details and the current checkout catalog, see: <http://www.itc.virginia.edu/training/cable/>

Online Information and Tips

Numerous vendor, news, and independent web sites provide non-technical information about computer security. The following two sites are examples:
Safe Internet: Microsoft Privacy and Security Fundamentals
<http://www.microsoft.com/privacy/safeinternet/>

ZDNet: Help and How To: PC Security Basics
<http://www.zdnet.com/zdhelp/stories/main/0,5594,2504682,00.html>

Training Sources for LSPs and System Administrators

Technical Training Contract Vendors

ITC-Training has entered into an agreement with three vendors to provide instructor-led Microsoft and Novell Technical Training Services to the University's computer professionals. Under the terms of the Agreement, the University can arrange for private classes or purchase seats available in public courses at preferential prices. All courses are official Microsoft or Novell courses. Details are available at:

<http://www.itc.virginia.edu/training/techtrain/index.htm>

School of Continuing and Professional Studies

The University's School of Continuing and Professional Studies, in conjunction with RRTC, offers a Certificate in Information Systems Management-Microsoft Systems. Information on this nine-course program can be found

at:<http://uvace.virginia.edu/rrtc/index.htm>

Piedmont Virginia Community College

PVCC offers courses in Microsoft, Novell, and Cisco technologies in the traditional, college credit format (through the Business Technologies Division), as well as a compressed, non-credit format through the college's Center for Training and Workforce Development. For details see: <http://www.pvcc.cc.va.us/cftwd/network.htm>

SANS Institute

For network and system administrators, the SANS Institute offers security courses online and in conjunction with their conferences. Course descriptions and costs can be found at the SANS site: <http://www.sans.org>

SAGE (System Administrators Guild)

SAGE is a technical group of the USENIX Association. The SAGE website (<http://www.usenix.org/sage>) provides information of interest to system administrators and security conferences sponsored by USENIX can be found at

<http://www.usenix.org/events/bytopic/security.html>

Appendix VI: Hiring Criteria

System administration is a widely varied task. The best systems administrators are generalists, combining technical knowledge, problem-solving ability, and interpersonal skills to support the goals of the department or group. The specific mix of skills and experience is dependent of the technology, size, and complexity of the systems being managed. The general criteria listed below can serve as a starting point for developing a department-specific set of criteria.

- Knowledge and experience with the hardware platforms used in the department.
- Solid understanding of the server operating system, including installation and configuration, network access, file management, and basic security provisions.
- Comfortable with most aspects of system administration, for example creation and maintenance of accounts, installation of applications, setup of network printers, and use of basic system administration tools and processes.
- Familiarity of fundamental network concepts and protocols, particularly TCP/IP
- Basic understanding of the common security threats faced by any Internet-connected organization.
- Strong inter-personal and communication skills, capable of interacting positively with users, management, and other IT professionals and groups, such as ITC.
- Ability to prioritize tasks and engage in independent problem solving
- Knowledge of backup technologies and procedure.
- Ability to identify tasks that require automation and implement automated solutions.

For additional information on the role of system administrators, particularly in a Unix/Linux environment, see The System Administrators Guild site:
<http://www.usenix.org/sage/jobs/jobs-descriptions.html>