

For:

- Students
- Instructors
- Researchers
- Staff
- IT Professionals

Responsibilities for Computing Devices Connected to the University of Virginia Network

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 noncompliance, 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.

- All device owners should ensure passwords used on their devices are not easily guessable by attackers.
- 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.
- 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.
- Owners of UNIX and Linux servers should switch off unneeded services to eliminate the risk of these being exploited.
- Owners of wireless access points and/or routers must insure that these devices do not allow unauthorized access to the University network.

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:

1. ITC or HS/CS, if the devices are under ongoing support contracts with these organizations;
2. 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;

UVa department heads, even in cases where vendor owned and/or managed equipment is housed in departments;

3. 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

Date/Revised Date:

July 1, 2001

Review Frequency:

Yearly by the Office of the VP/CIO

Help

- [Help Desk](#)
- [Request Help](#)
- [ITC How-to Guides](#)
- [Computer Terms Glossary](#)

About

- [ITC Services Directory](#)
- [Contact Us](#) • [Send Feedback](#)
- [Site Info](#) • Page Updated: 2005-09-28 EDT
- [© 2006 by the Rector and Visitors of the University of Virginia](#)

Standards & Policy

- [Disclaimer](#)
- [P3P Privacy Policy](#)
- Accessibility: [WAI](#) • [508](#)
- Web Standards: [XHTML](#) • [CSS](#)

University of Virginia
Information Technology and Communication
108 Cresap Road
P.O. Box 400217
Charlottesville, Virginia, 22904-4217 USA

Search for:



For:

- [Students](#)
- [Instructors](#)
- [Researchers](#)
- [Staff](#)
- [IT Professionals](#)

Statement on Obscene Material

University of Virginia

Based on statement from the General Counsel, Fall 1996

Although there may be difficult line-drawing in determining what is or is not obscene, students, faculty and staff should know that Va. Code Section 18.2-372 defines "obscene" as that which:

"Considered as a whole, has as its dominant theme or purpose . . . a shameful or morbid interest in nudity, sexual conduct, sexual excitement, excretory functions or products thereof or sadomasochistic abuse, and which goes substantially beyond customary limits of candor in description or representation of such matters and which, taken as a whole, does not have serious literary, artistic, political, or scientific value."

The distribution, production, publication or sale of obscene items is illegal in Virginia (Va. Code Section 18.2-374). A first offense is punishable as a Class 1 misdemeanor which carries a sentence of up to twelve months in jail and/or a fine of not more than \$2,500. Any subsequent obscenity conviction is a Class 6 felony which carries a sentence of between one and five years in prison, or up to twelve months in jail and/or a fine of \$2,500.

Further, a student, faculty or staff member distributing obscene material through a web page or other means could be subject to criminal prosecution in other states to the extent that any individual in those states accesses the web page or other delivery mechanism. Such action may violate federal law as well (18 U.S.C. Section 1465) which criminalizes the transportation of obscene materials in interstate commerce. Conviction under the federal law can result in a prison sentence of up to five years, a fine of not more than \$5,000, or both.

In addition, placing obscene material on a University of Virginia server violates University policies, including but not limited to the computer usage policy, the employee standards of conduct, and the student standards of conduct. Such violations could result in disciplinary penalties.

Help

- [Help Desk](#)
- [Request Help](#)
- [ITC How-to Guides](#)
- [Computer Terms Glossary](#)

About

- [ITC Services Directory](#)
- [Contact Us](#) • [Send Feedback](#)
- [Site Info](#) • Page Updated: 2005-09-28 EDT
- [© 2006 by the Rector and Visitors of the University of Virginia](#)

Standards & Policy

- [Disclaimer](#)
- [P3P Privacy Policy](#)
- Accessibility: [WAI](#) • [508](#)
- Web Standards: [XHTML](#) • [CSS](#)

University of Virginia
Information Technology and Communication
108 Cresap Road
P.O. Box 400217
Charlottesville, Virginia, 22904-4217 USA

© 2006 by the Rector and Visitors of the University of Virginia.

The information contained on the University of Virginia's Department of Information Technology and Communication (ITC) website is provided as a public service with the understanding that ITC makes no representations or warranties, either expressed or implied, concerning the accuracy, completeness, reliability or suitability of the information, including warranties of title, non-infringement of copyright or patent rights of others. These pages are expected to represent the University of Virginia community and the State of Virginia in a professional manner in accordance with the University of Virginia's Computing Policies.

Search for: **For:**

- [Students](#)
- [Instructors](#)
- [Researchers](#)
- [Staff](#)
- [IT Professionals](#)

Procedure for Revocation of Network Access

Information Technology and Communication University of Virginia

[FIRST APPROVED November 15, 1993; Revised July 22, 1996; Revised June 19, 1997, Revised May 1, 2000]

The Department of Information Technology and Communication (ITC) is neither an investigative nor a disciplinary entity in its primary responsibilities. However, in cases where University resources and privileges are abused or otherwise threatened, the department will take appropriate steps. The following is a procedure for action in such instances. The procedure applies only in cases involving ITC-owned or managed equipment. It does not apply to violations by ITC employees, which are covered by other processes.

1. ITC system administrators may revoke network access at any time to safeguard University resources and protect University privileges, as explained in the University-wide Computer Usage Policy, also known as the Ethics in Computer Usage statement. Such revocations will be for a maximum of one month, pending review by a committee appointed by the Vice President and Chief Information Officer (VP/CIO) of the University or his or her representative. This committee will report its decision to the VP/CIO; a request for review and/or appeal of the decision may be made to the VP/CIO.
2. The review committee appointed by the VP/CIO will include: at least one representative each of the instructional faculty, students, and classified staff, usually drawn from the membership of advisory committees to the Department of Information Technology and Communication or from ITC staff; the Director for Security Coordination and External Relations; and staff from the Vice President for Student Affairs Office.
3. The committee's duties include reviewing interim revocations by system administrators, extending such revocations to longer terms as it sees fit, and imposing sanctions in response to complaints it has received through the office of the VP/CIO. The committee bases its judgments on the University-wide Computer Usage Policy. The committee is also responsible for communicating the results of its review of such matters to appropriate authorities, generally the Vice President and Provost or the Vice President and Provost for the Health Sciences for faculty, the Vice President for Student Affairs for students, and the Director of Employee Relations for classified staff. If a person whose privileges

4. have been revoked then violates the conditions of the revocation, the next step of enforcement falls with those University officers. For example, a student who violates conditions of revocation risks charges under the student Standards of Conduct, especially Standard 12. Similar disciplinary mechanisms (beyond those of ITC) exist for faculty and classified staff.
5. As noted earlier, cases involving immediate threats to University resources and privileges may lead to interim action by ITC system administrators. System administrators or others (both within and beyond the University community) may lodge complaints against individual users whom they believe to have violated the University Computer Usage Policy. Those complaints will be made in writing or by e-mail to the VP/CIO at abuse@virginia.edu. ITC staff (coordinated by the VP/CIO) will assemble information about any case (either based on a complaint or on interim revocation of privileges by a system administrator) and will provide it to the committee.
6. The process for assembling information is as follows:
 1. A complaint or a notice of interim revocation by a system administrator comes to the VP/CIO's office in writing or by e-mail. The VP/CIO will review the matter to see if the alleged violation appears both intentional and serious enough to warrant committee review. If not, the matter ends here.
 2. The VP/CIO notifies the accused violator of the complaint in writing. That notice offers the accused violator the opportunity to provide a written response within a time limit (generally five working days) specified in the notice. The VP/CIO asks appropriate ITC staff and other University personnel to provide any additional information that would be useful in evaluating the case. The VP/CIO then gives the material to the committee, which makes its decision by majority vote on the basis of the records available. No hearing is involved.
 3. The accused violator is informed in writing of action taken. Copies of that notice are made for inclusion in the accused violator's file as noted in Section 2 (above). Appeals of the committee's decision may be made to the VP/CIO.
7. Sanctions that can be imposed by the committee range from a letter of warning to permanent revocation of network access. The committee will base the sanctions on the degree of potential harm created by the act and the degree of intent in the act, among other factors.
8. In any question of overlap to another disciplinary or law enforcement process, this process will defer to the other. In such cases, interim revocations by system administrators may remain in effect until the other process has been completed.

Help

- [Help Desk](#)
- [Request Help](#)
- [ITC How-to Guides](#)
- [Computer Terms Glossary](#)

About

- [ITC Services Directory](#)
- [Contact Us](#) • [Send Feedback](#)
- [Site Info](#) • Page Updated: 2005-09-28 EDT
- [© 2006 by the Rector and Visitors of the University of Virginia](#)

Standards & Policy

- [Disclaimer](#)
- [P3P Privacy Policy](#)
- Accessibility: [WAI](#) • [508](#)
- Web Standards: [XHTML](#) • [CSS](#)

University of Virginia

Information Technology and Communication

108 Cresap Road

P.O. Box 400217

Charlottesville, Virginia, 22904-4217 USA

For:

- [Students](#)
- [Instructors](#)
- [Researchers](#)
- [Staff](#)
- [IT Professionals](#)

Statement on Privacy of, Access to, and Retention of Computer Files

University of Virginia
May 10, 1993

The University regards electronic mail and voice communications as vehicles for delivery of information and not as mechanisms for the retention or archiving of such information.

It is the responsibility of the individual sender and/or receiver of such messages to determine which information should be retained or archived. Records should be retained in accordance with the University's financial and administrative policy on records retention and disposition (policy # II.C.1) and the Virginia state code. Records that are retained by an individual, even if they are retained on an electronic medium, are subject to the Virginia Freedom of Information Act and the Privacy Act. Current electronic technology is not considered acceptable for archival storage. Thus, documents judged to be archival should be stored on an appropriate medium such as paper or microfilm.

Users of computer systems are expected to abide by the guidelines on "Ethics in Computer Usage."

Help

- [Help Desk](#)
- [Request Help](#)
- [ITC How-to Guides](#)
- [Computer Terms Glossary](#)

About

- [ITC Services Directory](#)
- [Contact Us](#) • [Send Feedback](#)
- [Site Info](#) • Page Updated: 2005-09-28 EDT
- [© 2006 by the Rector and Visitors of the University of Virginia](#)

Standards & Policy

- [Disclaimer](#)
- [P3P Privacy Policy](#)
- Accessibility: [WAI](#) • [508](#)
- Web Standards: [XHTML](#) • [CSS](#)

University of Virginia
Information Technology and Communication
108 Cresap Road
P.O. Box 400217
Charlottesville, Virginia, 22904-4217 USA

Search for:



For:

- [Students](#)
- [Instructors](#)
- [Researchers](#)
- [Staff](#)
- [IT Professionals](#)

University of Virginia Policy on Monitoring/Review of Employee Electronic Communications or Files

FINAL DRAFT 10/03/01

Developed by the University of Virginia Office of Information Technologies

Policy Authority and Effective Date	Pending final approval by the Exec. VP and COO; responsible office is Office of Information Technologies; interim effective date is 10/03/01
Affects	All employees of the University
Subject/Purpose	Defines University policy on institutional monitoring or review of the content of employee electronic communications or employee electronic files
Policy text	<p>The Commonwealth of Virginia's Human Resource Policy 1.75 contains the following statement: "No user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the Commonwealth's equipment and/or access." The policy states that Virginia agencies, including its institutions of higher education, have "the right to monitor any and all aspects of their computer systems" and to do so "at any time, without notice, and without the user's permission." The policy applies to all state employees, including faculty and staff of the University of Virginia.</p> <p>The University holds as core values the principles of academic freedom and free expression. In consideration of these principles, the University will not monitor the content of electronic communications of its employees in most instances, nor will it examine the content of employee electronic communications or other employee electronic files stored on its systems except under certain circumstances. In this context, "electronic communications" includes telephone communications, so-called "phone mail," e-mail, and computer files traversing the University network or</p>

stored on University equipment.

Examples of when monitoring and/or review may occur include, but are not limited to, the following circumstances:

- communications or files targeted by orders of a court of law or requested in accord with the Virginia Freedom of Information Act.
- supervisor and/or Internal Audit review of University telephone system long distance call records.
- electronic communications or files that have been inadvertently exposed to technical staff who are operating in good faith to resolve technical problems. When technical staff inadvertently see or hear potentially illegal content in communications or files, they are required to report what they have seen or heard to appropriate authorities. Otherwise, the University expects technical staff to treat inadvertently encountered electronic communications and files of University employees as confidential and not subject to disclosure to anyone.
- routine administrative functions, such as security tests of computing systems, including password testing by system administrators to identify guessable passwords, and investigations of attempted access into systems by unauthorized persons (system administrators and other technical staff will not access employees' electronic communications or files while performing these functions).
- situations such as:
 - an investigation into allegations of violations of law or policy
 - an urgent need for access to University business documents when an employee is unavailable

Such situations will be specifically reviewed by and approved by the president or the vice president (or equivalent) responsible for the affected employee(s).

- for some units of the University, routine monitoring or examination of employee electronic communications or files as part of the work environment. Such routines must be approved by the relevant vice president (or equivalent), and affected employees must be informed in advance that such monitoring or examination will be taking place.

This policy does not mean that the University has lower expectations for its employees' behavior. It expects University employees to obey all applicable policies and laws in the use of computing and communications technologies.

See related [Guidance document](#).

Help

- [Help Desk](#)
- [Request Help](#)
- [ITC How-to Guides](#)
- [Computer Terms Glossary](#)

About

- [ITC Services Directory](#)
- [Contact Us](#) • [Send Feedback](#)
- [Site Info](#) • Page Updated: 2005-09-28 EDT
- [© 2006 by the Rector and Visitors of the University of Virginia](#)

Standards & Policy

- [Disclaimer](#)
- [P3P Privacy Policy](#)
- Accessibility: [WAI](#) • [508](#)
- Web Standards: [XHTML](#) • [CSS](#)

University of Virginia
Information Technology and Communication
108 Cresap Road
P.O. Box 400217
Charlottesville, Virginia, 22904-4217 USA