Virginia Union University's Computing Policies

The following Virginia Union University policies apply to the entire university community. The policies address the responsible use of information and technology resources, violations of policy and guidelines for effective use of technology resources. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and guidelines are subject to change as technologies, state, and federal laws develop and change. Please check back often for any updates or changes.

Contents:

Area of Responsibility: OFFICE OF INFORMATION TECHNOLOGY

Responsible Contact: DIRECTOR OF INFORMATION TECHNOLOGY

Policy Identification: TENETS OF RESPONSIBLE COMPUTING - SECTION 11.1

Effective Date: JANUARY 2009

Everyone within the Virginia Union University community who uses University computing and network facilities has the responsibility to use them in an ethical, professional, and legal manner.
Users agree to abide by the following conditions:

Access to Virginia Union University technology resources are limited to current Students, Faculty, and Staff. VUU's internal resources and services are not provided to outside organizations or individuals other than access to our VUU-Guest-WIFI network for internet access only.

Use the University's computing facilities and information resources, including hardware, software, networks, and computer accounts, responsibly and appropriately.

Respect the rights of other computing users, and respect all contractual and license agreements.

Use only those computers and computer accounts for which you have authorization.

The University's network and computer infrastructure is a finite resource. Use computer accounts for the purpose(s) for which they have been issued. Use University owned computer systems for University-related projects only. Commercial use of the University's computing resources, not related to the academic, research, and scholarly pursuits is prohibited.

Be responsible for all computer accounts and for protecting each account's password. In other words, do not share computer accounts. If someone else learns your password, you must change it.
Report unauthorized use of your account to your department director, instructor, supervisor, system administrator, or other appropriate University authority.

During an investigation of a problem, cooperate with Information Services' requests for information about computing activities.

Do not participate in the malicious use of computing resources.

Users of VUU's equipment, services, network, and resources should have no expectation of privacy

Report any abuse of computing resources to the Office of Information Technology Immediately.

Area of Responsibility: OFFICE OF INFORMATION TECHNOLOGY

Responsible Contact: DIRECTOR OF INFORMATION TECHNOLOGY

Policy Identification: COMPUTING VIOLATIONS - SECTION 11.2

Effective Date: JANUARY 2009

Examples of prohibited actions (not a comprehensive list) that are subject to disciplinary review are:

Attacking the security of the system or failing to maintain the security of the system;

Using obscene or abusive language in electronic communications;

Harassing, threatening or otherwise causing harm to specific individuals, e.g., sending an individual repeated and unwanted (harassing) email or using email to threaten or stalk someone;

Accessing or attempting to access another individual's data or information without proper authorization, e.g., running an unauthorized remote control of another's computer;

Tapping phone or network lines, e.g., running network sniffers without authorization;

Releasing a virus, worm or other program that damages or harms a system or network;

Preventing others from accessing services;

Sending pyramid or chain letters over the network;

Accessing data or files without authorization, even if they are not securely protected, e.g. taking advantage of security holes;

Modifying or divulging private information such as electronic files or the contents of mail without the consent of the owner of the files

Using or misusing of University electronic data without authorization;

Modifying, damaging, defacing, moving or destroying data which does not belong to you;

Using the national network, the internet, in a manner contrary to established guidelines and laws;

Downloading or posting to university computers, or transporting across the university networks, material that is illegal, proprietary, in violation of university contracts, or otherwise damaging to the institution, e.g., launching a computer virus, distributing child pornography, posting copyright or contract protected information.

Violations of federal, state, or local laws.

The underlying premise of the above policy is:

The legitimate use of a computer or a network does not extend to whatever an individual is capable of doing with it. Just because a person is able to circumvent restrictions and security, this does not mean that the person is allowed to do so.

Area of Responsibility:	**OFFICE OF INFORMATION TECHNOLOGY**
Responsible Contact:	**DIRECTOR OF INFORMATION TECHNOLOGY**
Policy Identification:	**HANDLING VIOLATIONS - SECTION 11.3**
Effective Date:	**JANUARY 2009**

The primary responsibilities of the Office of Information Technology are neither investigative nor disciplinary; however, in cases where University resources and privileges are abused or otherwise threatened, the staff in the offices will take appropriate steps.

In all cases where a member of the University community allegedly has committed one of the above violations, the Office of Information Technology will immediately revoke access privileges pending the outcome of a full review of the problem.

The person will be notified as quickly as possible, by phone, electronic, campus or U.S. mail of the alleged violation. A representative of the Office of Information Technology staff will contact the person to propose a meeting to discuss the alleged violation.

If the issue cannot be resolved, and depending on the nature of the alleged offense, the Office of Information Technology will contact the appropriate senior university administrator (Director of Human Resources, Dean, Vice President, Campus Police) or law enforcement agencies alerting them of the alleged violation and conferring on the proper next steps.

In all cases, if the problem in question overlaps with 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.

Once a formal complaint is made, the University shall protect the confidentiality of those involved to the extent permitted by law and to the extent that continued protection does not interfere with the University's ability to investigate allegations and to take corrective action.

Area of Responsibility:	**OFFICE OF INFORMATION TECHNOLOGY**
Responsible Contact:	**DIRECTOR OF INFORMATION TECHNOLOGY**
Policy Identification:	**SOFTWARE COPYRIGHT POLICY - SECTION 11.4**
Effective Date:	**JANUARY 2009**

NOTE: This Section was developed as part of Virginia Union University's efforts to comply with the Higher Education Opportunity Act (HEOA) and 34 CFR Sec. 668.14(b)(30).

Federal copyright laws protect the software available for use on computers at Virginia Union University. Educational institutions are not exempt from the laws covering copyright. In addition, software is normally protected by a license agreement between the purchaser and the software seller. The software provided through the University for use by faculty, staff, and students may be used only on computing equipment as specified in the various software licenses.

It is University policy to respect the copyright protections given to software and intellectual property owners by federal law. The University recognizes that the purpose of copyright is to protect the rights of the creators of intellectual property and to prevent the unauthorized use or sale of these works. It is against University policy for faculty, staff, or students to copy or reproduce any licensed software or intellectual property on University computing equipment, except as expressly permitted by the software license or granting authority. Faculty, staff, and students may not use copies of software that have been obtained illegally, on University-owned Computers, Information systems, Networks and other Information Technology resources. Or on personal Computers using Virginia Union University's Networks and other Information Technology resources.

You may not use Virginia Union University networks, equipment and software to violate copyright or the terms of any license agreement

Unauthorized Peer-to-Peer file sharing is illegal and is regarded as a serious matter and any such use is without the consent of Virginia Union University and is subject to disciplinary action by the appropriate division in the university and termination of network access

The unauthorized distribution of copyrighted material such as songs, videos, games, textbooks, or other types of creative content, including through peer-to-peer file sharing, is prohibited by Virginia Union University policy and may violate civil or criminal law.

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.

Legal Alternatives

EDUCAUSE maintains a list of known Legal Alternatives: legitimate download services. http://www.educause.edu/legalcontent

Area of Responsibility:	**OFFICE OF INFORMATION TECHNOLOGY**
Responsible Contact:	**DIRECTOR OF INFORMATION TECHNOLOGY**
Policy Identification:	**E-MAIL GUIDELINES: PRIVACY AND ETIQUETTE - SECTION 11.5**
Effective Date:	**JANUARY 2009**

Access to Virginia Union University email system is limited to current Students, Faculty, and Staff. VUU's email services are not provided to outside organizations or individuals

E-mail messages are written records that could be subject to review with just cause. Courts have also ruled that e-mail records and information in electronic form on network computers can be subpoenaed. Under present circumstances, the privacy of e-mail cannot be guaranteed. Users should not maintain any expectations of privacy.

University policy establishes the privacy of the messages and the files on the network computers. However, when we experience system problems, such as hardware or software failure or attacks by malicious users, the ITC staff members who maintain the mail servers are authorized to look at any information and any files on university computers that are necessary to solve the problems and to protect the systems and the information they contain. It is part of the system administrator's job to do this and to treat any information on the systems as confidential.

While the University respects faculty, staff and students privacy to all reasonable limits, the University and/or the Office of Information Technology cannot guarantee that all email will remain private. In addition to the authorized actions of system administrators, e-mail can end up in the hands of computing staff if it was inaccurately addressed and if it could not be delivered. People also make small mistakes in addressing their mail so that private messages appear in the mailbox of someone other than the intended recipient.

University policies prohibit certain kinds of e-mail messages. Policies prohibit using email for harassment, political campaigning, and solicitation. Chain mail is an irresponsible use of resources, and it taxes the network; therefore, sending chain mail is a violation of policy. VUU email users must not employ a false identity when sending email, applying for an email account, or accessing an account

Area of Responsibility: **OFFICE OF INFORMATION TECHNOLOGY**

Responsible Contact: **DIRECTOR OF INFORMATION TECHNOLOGY**

Policy Identification: **PROTECTING UNIVERSITY INFORMATION - SECTION 11.6**

Effective Date: **JANUARY 2009**

Many systems at the University require the use of passwords. These include email, Campus Web (My.VUU intranet), labs and classrooms. Although each of these systems has its own requirements, they all share the requirement that passwords be kept protected to prevent any unauthorized use. It is important that you choose a good password and keep it secret from everyone. No one should be given your password -- not even someone from the Office of Information Technology You should change your password regularly, and will be required to change it every 120 days. You should change your password immediately if you notice unusual activity on your system or account. If you suspect that someone is illegally accessing computing resources using your identity, please contact the ITC Help Desk at 257-5630.

Area of Responsibility:	**OFFICE OF INFORMATION TECHNOLOGY**
Responsible Contact:	**DIRECTOR OF INFORMATION TECHNOLOGY**
Policy Identification:	**STATEMENT ON OBSCENE MATERIAL - SECTION 11.7**
Effective Date:	**JANUARY 2009**

While Virginia Union University is a private university, all members of the community still must observe state and federal laws. Although it may be difficult to draw the line in determining what is or is not obscene, students, faculty and staff should know that Virginia 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 that 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 that 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 makes the transportation of obscene materials in interstate commerce a criminal act. Conviction under 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 Virginia Union University server violates University policies, including but not limited to the computer usage policy as well as employee and student standards of conduct. Such violations will result in disciplinary actions.

Area of Responsibility:	**OFFICE OF INFORMATION TECHNOLOGY**
Responsible Contact:	**DIRECTOR OF INFORMATION TECHNOLOGY**
Policy Identification:	**UNIVERSITY TECHNOLOGY RESOURCES OWNERSHIP - SECTION 11.8**
Effective Date:	**JANUARY 2009**

The University owns the network computers, computer labs, the micro-computing sites, and the computers issued to and places on its staff and faculty desks, Labs and all the software it has installed on them. The University owns the campus network - all wires, cables, and routers that connect the personal computers, central computers, computer labs, microcomputer sites, and servers to each other and to the Internet.

Access to Virginia Union University technology resources are limited to current Students, Faculty, and Staff. VUU's internal resources and services are not provided to outside organizations or individuals other than access to our VUU-Guest-WIFI network for internet access only. The University's Office of Information Technology determines who is authorized to use its network.

While Virginia Union University owns the computers in all the offices, labs and departments, each individual staff member is responsible how that equipment will be used. The University also owns the software licenses (word processing, spreadsheet software, email, etc.) that were purchased from a software vendor using university funds. The licenses usually allow ONE copy of this software per workstation unless otherwise licensed.

The University can't give unlimited space to store email. Cleaning out mailboxes is a task that should be practiced regularly. VUU will only store up to six months of email.

Virginia Union University owns all the technology equipment and reserves the right to inspect, examine and monitor the use of its computers, computer networks, e-mail systems, telephone systems, and all electronic communication systems attached or connected to the Universities wireless or wired network at any time without notice. Users of VUU's equipment, services, network, and resources should have no expectation of privacy

Area of Responsibility:	**OFFICE OF INFORMATION TECHNOLOGY**
Responsible Contact:	**DIRECTOR OF INFORMATION TECHNOLOGY**
Policy Identification:	**FOREIGN INVADERS: VIRUSES - SECTION 11.9**
Effective Date:	**JANUARY 2009**

Computer viruses are segments of program code that interfere with the running of the programs and with access to data on a computer. The virus code resides on a diskette or on another computer system on a network. When the virus code is copied from the diskette or from another computer system over the network, it infects the system it is copied onto. In 1988, there were less than a dozen computer viruses in existence. The number of virus definitions from McAfee for 2008 is expected to reach 400,000 the total number of viruses is projected to reach 1 million by the end of 2009, according to security experts.

Many viruses are more of a nuisance than an actual cause of damage to the computer system or data. One virus simply prints "Don't panic" on the screen. Many other viruses, however, destroy data and render computer systems inoperable. The Michelangelo virus overwrites the hard disk. The Jerusalem virus deletes executable files. Some viruses called "rabbits" just reproduce, eventually taking up all processor capacity, memory, and disk, denying the user access to system resources. Word processor and spreadsheet macro viruses are another threat. Some viruses serve as Trojan Horses and open your computer up to external and illegal users. Installing or knowingly proliferating viruses in any format is a serious violation of university policy and is subject to disciplinary action by the appropriate authorities in the university.

Area of Responsibility:	OFFICE OF INFORMATION TECHNOLOGY
Responsible Contact:	DIRECTOR OF INFORMATION TECHNOLOGY
Policy Identification:	WHAT TO DO IF YOU ARE A VICTIM OF COMPUTER ABUSE, HARASSMENT OR IRRESPONSIBLE BEHAVIOR-SECTION 11.10
Effective Date:	JANUARY 2009

Unfortunately computer abuse, harassment, malicious behavior, and unauthorized account access do happen. If you are a victim of computer abuse, report the violations to, an administrator, your supervisor, Campus Police or Information Services. Please keep copies of the harassing e-mail messages, dates, and times of unauthorized access, etc., for investigative purposes. Cases are handled in accordance with the university's harassment policy and in the utmost confidentiality.

The University shall protect the confidentiality of those involved to the extent permitted by law and to the extent that continued protection does not interfere with the University's ability to investigate allegations and to take corrective action.