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. Suggestions on these policies are welcomed and should be sent to the Director for Information Technology.

Contents:

I. The Virginia Union University Policy on Responsible Computing

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.

This means that users agree to abide by the following conditions:

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

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

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

o 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.

o 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.

o Report unauthorized use of your accounts to your project director, instructor, supervisor, system administrator, or other appropriate University authority.

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

o Do not participate in the malicious use of computing resources.

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

II. Computing Violations

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

o Attacking the security of the system or failing to maintain the security of the system;
o Using obscene or abusive language in electronic communications;
o 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;
o 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;
o Tapping phone or network lines, e.g., running network sniffers without authorization;
o Releasing a virus, worm or other program that damages or harms a system or network;
o Preventing others from accessing services;
o Sending pyramid or chain letters over the network;
o Accessing data or files without authorization, even if they are not securely protected, e.g. taking advantage of security holes;
o Modifying or divulging private information such as electronic files or the contents of mail without the consent of the owner of the files
o Using or misusing of University electronic data without authorization;
o Modifying, damaging, defacing, moving or destroying data which does not belong to you;

o Using the national network, the internet, in a manner contrary to established guidelines and laws;
o 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 via the web, posting copyright or contract protected information.
o 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.

III. The Virginia Union University Policy and Procedures on Handling Violations
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.

IV. The Virginia Union University Software and Intellectual Property Copyright Policy

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. 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 or on personal computers housed in University facilities.

Unauthorized use of software 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.

V. E-mail Guidelines: Privacy and Etiquette

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 in some cases. 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

Some hints and guidelines on email:

- Just like written letters, the receiver owns the e-mail messages. They can easily be redistributed or copied by the recipients.

- Realize that University policy and secure passwords provide good but not complete assurance of the privacy of e-mail messages. When the confidentiality of a message is of the utmost importance, only a person-to-person conversation may be sufficiently secure.
- Delete redundant and unwanted messages that should not be preserved
- Delete sent messages and empty the deleted Items folder regularly
- Resist the temptation to send chain mail, even when it promises you fame and fortune Any message that has been forwarded ten or more times is a chain letter. This is a waste of computing resources, it's a nuisance, and it often offends recipients
- Don't use University resources, computing or otherwise, for political campaigning or soliciting.
- Only use University resources, for Virginia Union University authorized business

VI. Securing Passwords; Protecting Files; Protecting University Information

Many systems at the University require the use of passwords. These include email, the Web, labs in Library, and others. Although each of these systems has its own requirements, they all share the requirement that passwords be kept protected to prevent any unauthorized use.

The Importance of Password Protection

Your login ID and password authenticate you as an authorized user of Virginia Union University's computing environment. A good password policy is key to the University's overall systems security. You need to protect your own files and University resources by choosing a good password and protecting it.

If another person discovers your password, that individual potentially has access to your email, your personal files, and your online network identity and accounts. A knowledgeable person could use your account to illegally gain access to other network resources putting them at risk. Part of a strong defense against intruders is a good secure password.

Hackers often gain access to a system by "cracking" accounts. They use automated processes to guess passwords. This process is quick and easy for them if you use a dictionary word or your login ID for a password. You should change your password regularly, and will be required to change it every 90 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.

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

The Office of Information Technology may run a program from time to time that looks across our systems for “crackable” passwords. If we find one on your account we will ask

you to change it immediately. We will also put procedures in place that will prevent users from selecting insecure passwords where possible.

If passwords are created intelligently and kept protected, the danger is minimized; but if an employee and/or student is not careful to protect his or her password, that employee and/or student can permit an unscrupulous person access to a valuable University asset: its information.

How to Choose a Good Password
The University's policy for choosing a good (that is, less hackable) password requires the following for all systems:

o Do not use "dictionary words" (even if they are "disguised" by capital letters or numbers, like 'RiCHmonD' or 'birthday98'), foreign words, names, dates, phone numbers or anything else someone might be able to simply guess or determine using a hacking tool.
o You are required to use a minimum of six characters or more using less makes the password too easy to hack or guess. Use at least two letters and at least one non-letter (number or special character), but the first character in the password must be a letter.
o Make your password easy for you to remember, but hard for someone else to guess. Picking letters from a phrase that's meaningful to you may make a good password. An example could be "Fall 98 classes begin on August 25" becomes f9cboA2.
o Intersperse numbers, punctuation marks and special characters. Allowable special characters are: @ # $ % ^ & * ( ) _ - + = { } [ ] \ : ; " ? ' / > . < ,
o Use a unique password. Do not use one that you are using for some other purpose, such as your PIN at your bank or your password to another University system.

How to Protect Your Password
o You should never write your password down! However, if you must write it down be sure to store it where no one else will see it.
o Do not put it on or near your computer, in the front of your Rolodex (or filed under "P"), or in your desk drawer. Put it somewhere where no one but you will have access to it, such as in your wallet. There is no reason for anyone but you to ever have access to your passwords, so there is no reason to share them with anyone in your office.

Change your password occasionally. Change it when:
o You have told it to anyone, or have written it down and think it may have been observed;
o You have used the same password for more than Three months;
o Your password does not meet the criteria for a good password in this policy;
o You are advised by ITC or your system administrator to change it;
o You have reason to suspect the password has been compromised.

If You Forget your Password
o Contact the Help Desk at extension 5630.

VII. The Virginia Union University Statement on Obscene Material

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.

VIII. University Technology Resources: Ownership

The University owns the network computers, computer labs, the micro-computing sites, and the computers it places on its staff and faculty desks 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. 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 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.

Also, the University can't give unlimited space to store email. Cleaning out mailboxes is a task that should be practiced regularly.

IX. Foreign Invaders: Viruses

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 will 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.

Hints and guidelines on computer viruses:

o Be suspicious of freeware and shareware. Be wary of downloading files from electronic bulletin boards.

o Back up, store, and routinely check backup copies of all files and programs. Keep the backups for as long as six months to a year.

o Use anti-virus software. For all computers

X. What to do if You are a Victim of Computer Abuse, Harassment or Irresponsible Behavior

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.

A downloadable version of the above document can be downloaded from http://www.vuu.edu/Technology/VirginiaUnionUniversityComputerPolicies.pdf