VCCS Computer Ethics Policy

Thousands of customers share VCCS information technology resources. Everyone must use these resources responsibly since misuse by even a few individuals has the potential to disrupt VCCS business or the work of others. Therefore you must exercise ethical behavior when using these resources.

State Law (Article 7.1 of Title 18.2 of the Code of Virginia) classifies damage to computer hardware or software (18.2-152.4), unauthorized examination (18.2-152.5), or unauthorized use (18.2-152.6) of computer systems as misdemeanor crimes. Computer fraud (18.2-152.3) and use of a computer as an instrument of forgery (18.2- 152.14) can be felonies. VCCS internal procedures for enforcement of its policy are independent of possible prosecution under the law.

Definition

VCCS information technology resources include mainframe computers, minicomputers, microcomputers, networks, software, data, facilities and related supplies.

Guidelines

The following guidelines shall govern the use of all VCCS information technology sources.

You must use only those computer resources that you have the authority to use. You must not provide false or misleading information to gain access to computing resources. The VCCS may regard these actions as criminal acts and may treat them accordingly. You must not use these resources to gain unauthorized access to computing resources of other institutions, organizations or individuals.

1. You must not authorize anyone to use your computer accounts for any reason. You are responsible for all use of your accounts. You must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of your account by unauthorized persons. You must not, for example, share your password with anyone.
2. You must use your computer resources only for authorized purposes. Students or staff, for example, may not use their accounts for private consulting. You must not use your computer resources for unlawful purposes, such as the installation of fraudulently or illegally obtained software. Use of external networks connected to the VCCS information technology resources must comply with the policies of acceptable use promulgated by the organizations responsible for those networks.
3. Other than material known to be in the public domain, you must not access, alter, copy, move or remove information, proprietary software or other files (including programs, members of subroutine libraries, data and electronic mail) without prior authorization. The College or VCCS data trustee, security officer, appropriate college official or other responsible party may grant authorization to use electronically stored materials in accordance with policies, copyright laws and procedures. You must not copy, distribute or disclose third party proprietary software without prior authorization from the licenser. You must not install proprietary software on systems not properly licensed for its use.
4. You must not use any computing facility irresponsibly or needlessly affect the work of others. This includes:
    - Transmitting or making accessible offensive, annoying or harassing material;
    - Intentionally, recklessly, or negligently damaging systems;
    - Intentionally damaging or violating the privacy of information not belonging to you;
    - Intentionally misusing resources or allowing misuse of resources by others;
    - Loading software or data from untrustworthy sources onto official systems without prior approval.

You should report any violation of these regulations by another individual and any information relating to a flaw or bypass of computing facility security to the Information Security Officer or the Internal Audit department.

Enforcement Procedures

1. Faculty, staff and students at the college or VCCS should immediately report violations of information security policies to the local Chief Information Officer (CIO) who will research the information about the case and identify the offender. If state or federal law is apparently violated then the research shall be conducted in conjunction with appropriate legal authorities in order to protect legal evidence.
2. The College president will report any alleged violations of state and federal law to the appropriate authorities.
3. If the alleged offender is an employee, the CIO will notify the offender's supervisor. The supervisor,

in conjunction with the College or System Human Resources officer and the CIO will follow the Human Resource published procedure for adjudication of the alleged violation.

4. If the alleged offender is a student, the CIO will notify the vice president of finance and administration. The vice president, in cooperation with the CIO, will follow the published student procedure for adjudication of the alleged violation.
5. All formal disciplinary findings and actions taken under this policy may be pursued by the accused through the appropriate grievance procedure.

The VCCS Computer Ethics Guidelines shall remain in effect from November 30, 2000 until superseded or suspended.

Information Technology Student/Patron Acceptable Use Agreement

Version:
3.1
Status: Approved 06/16/2010
Contact: Director, Technology Administration Services

As a user of the Virginia Community College System's local and shared computer systems, I understand and agree to abide by the following acceptable use agreement terms. These terms govern my access to and use of the information technology applications, services and resources of the VCCS and the information they generate. The college has granted access to me as a necessary privilege in order to perform authorized functions at the college where I am currently enrolled. I will not knowingly permit use of my entrusted access control mechanism for any purposes other than those required to perform authorized functions related to my status as a student. These include logon identification, password, workstation identification, user identification, digital certificates or 2-factor authentication mechanisms.

I will not disclose information concerning any access control mechanism unless properly authorized to do so by my enrolling college. I will not use any access mechanism that the VCCS has not expressly assigned to me. I will treat all information maintained on the college computer systems as strictly confidential and will not release information to any unauthorized person.

Computer software, databases, and electronic documents are protected by copyright law. A copyright is a work of authorship in a tangible medium. Copyright owners have the sole right to reproduce their work, prepare derivatives or adaptations of it, distribute it by sale, rent, license lease, or lending and/or to perform or display it. A student must either have an express or implied license to use copyrighted material or data, or be able to prove fair use. Students and other users of college computers are responsible for understanding how copyright law applies to their electronic transactions. They may not violate the copyright protection of any information, software, or data with which they come into contact through the college computing resources. Downloading or distributing copyrighted materials such as documents, movies, music, etc. without the permission of the rightful owner may be considered copyright infringement, which is illegal under federal and state copyright law. Use of the college's network resources to commit acts of copyright infringement may be subject to prosecution and disciplinary action.

The penalties for infringing copyright law can be found under the U.S. Copyright Act, 17 U.S.C. §§ 501- 518 (http://www.copyright.gov/title 17/92chap5.html) and in the U.S. Copyright Office's summary of the Digital Millennium Copyright Act (http://www.copyright.gov/legislation/dmca.pdf).

I agree to abide by all applicable state, federal, VCCS, and college policies, procedures and standards that relate to the Virginia Department of Human Resource Management Policy 1.76-Use of Internet and Electronic Communication Systems, the VCCS Information Security Standard and the VCCS Information Technology Acceptable Use Standard. These include, but are not limited to:

- Attempting to gain access to information owned by the college or by its authorized users without the permission of the owners of that information.
- Accessing, downloading, printing, or storing information with sexually explicit content as prohibited by law or policy;
- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images;
- Installing or downloading computer software, programs, or executable files contrary to policy;

- Uploading or downloading copyrighted materials or proprietary agency information contrary to policy;
- Sending e-mail using another's identity, an assumed name, or anonymously;
- Attempting to intercept or read messages not intended for them;
- Intentionally developing or experimenting with malicious programs (viruses, worms, spy-ware, keystroke loggers, phishing software, Trojan horses, etc.) on any college-owned computer;
- Knowingly propagating malicious programs;
- Changing administrator rights on any college-owned computer, or the equivalent on non-Microsoft Windows based systems;
- Using college computing resources to support any commercial venture or for personal financial gain.

Students must follow any special rules that are posted or communicated to them by responsible staff members, whenever they use college computing laboratories, classrooms, and computers in the Learning Resource Centers. They shall do nothing intentionally that degrades or disrupts the computer systems or interferes with systems and equipment that support the work of others. Problems with college computing resources should be reported to the staff in charge or to the Information Technology Help Desk.

If I observe any incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the Information Security Officer and/or management of my college.

I understand that I must use only those computer resources that I have the authority to use. I must not provide false or misleading information to gain access to computing resources. The VCCS may regard these actions as criminal acts and may treat them accordingly. I must not use VCCS IT resources to gain unauthorized access to computing resources of other institutions, organizations, individuals, etc. The System Office and colleges reserve the right (with or without cause) to monitor, access and disclose all data created, sent, received, processed, or stored on VCCS systems to ensure compliance with VCCS policies and federal, state, or local regulations. College or System Office officials will have the right to review and/or confiscate (as needed) any equipment (COV owned or personal) connected to a COV owned device or network. I understand that it is my responsibility to read and abide by this agreement, even if I do not agree with it. If I have any questions about the VCCS Information Technology Acceptable Use Agreement, I understand that I need to contact the college Information Security Officer or appropriate college official.

By acknowledging this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that should I violate this agreement, I will be subject to disciplinary action.