



Information Technology Acceptable Use Guideline

Version: 1.0
Status: Approved 3/31/04
Contact: [James Davis](#)

Thousands of users 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. The VCCS's internal procedures for enforcement of its policy are independent of possible prosecution under the law.

DEFINITION

VCCS information technology resources include mainframe computers, servers, desktop computers, notebook computers, handheld devices, networks, software, data files, facilities, and the related supplies. .

GUIDELINES

The following guidelines shall govern the use of all VCCS information technology resources:

1. 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 VCCS IT resources to gain unauthorized access to computing resources of other institutions, organizations or individuals.
2. 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.
3. 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 any VCCS facility must comply with the policies of acceptable use promulgated by the organizations responsible for those networks.

4. 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 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 licensor. You must not install proprietary software on systems not properly licensed for its use.

5. 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. This includes intentionally, recklessly, or negligently damaging systems, intentionally damaging or violating the privacy of information not belonging to you. This includes the intentional misuse of resources or allowing misuse of resources by others. This includes loading software or data from untrustworthy sources, such as free-ware, onto official systems without prior approval.

6. 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 Office or the Internal Audit department.

ENFORCEMENT PROCEDURE

1. Faculty, staff and students at the college or System Office should immediately report violations of information security policies to the local Chief Information Officer (CIO).

2. If the accused is an employee, the CIO will collect the facts of the case and identify the offender. If, in the opinion of the CIO, the alleged violation is of a serious nature, the CIO will notify the offender's supervisor. The supervisor, in conjunction with the College or System Human Resources Office and the CIO, will determine the appropriate disciplinary action. Disciplinary actions may include but are not limited to:

a. Temporary restriction of the violator's computing resource access for a fixed period of time, generally not more than six months.

b. Restitution for damages, materials consumed, machine time, etc. on an actual cost basis. Such restitution may include the cost associated with determining the case facts.

c. Disciplinary action for faculty and classified staff in accordance with the guidelines established in the State Standards of Conduct Policy.

3. In the event that a student is the offender, the accuser should notify the Vice President of Instruction. The VP, in cooperation with the CIO, will determine the appropriate disciplinary actions which may include but are not limited to:

- a. Temporary restriction of the violator's computing resource access for a fixed period of time, generally not more than six months.
- b. Restitution for damages, materials consumed, machine time, etc. on an actual cost basis. Such restitution may include the cost associated with determining the case facts.
- c. Disciplinary action for student offenders shall be in accordance with the college student standards of conduct.

4. The College President will report any violations of state and federal law to the appropriate authorities.

5. All formal disciplinary actions taken under this policy are subject to the commonwealth's personnel guidelines and the accused may pursue findings through the appropriate grievance procedure.