Technology Standard

Personnel Security ± Acceptable Use

Version: 1.0
Status: Approved: 02/21/07
Contact: Director, Technology Services

PURPOSE

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), invasion of privacy (18.2-152.5), or theft of computer services (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.

SCOPE

In accordance with the COV ITRM 501-01, Acceptable Use requirements define acceptable and permitted use of COV, VCCS, and college IT resources.

APPLICABILITY

The Acceptable Use Standard is applicable to the System Office and all Colleges.

DEFINITION

VCCS information technology resources include mainframe computers, servers, desktop

This includes loading software or data from untrustworthy sources, such as free software, onto official systems without prior approval.

9. 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.

10. < R X P X V W Q R W X V H W K H & R P P R Q Z H D O W K ¶ V Q H W Z R U N I R U D Q \ S X U S R V H W K D W L V Q R W U H O D W H G W R W K H E X V L Q H V V R U I X Q F W L R Q L Q J R I W K H D J H Q F \ R U W K H & R P P R Q Z H D O W K L Q F O X G L Q J W K R V H F D V H V Z K H U H L W :

x L Q W H U I H U H V Z L W K W K H X V H U ¶ V S U R G X F W L Y L W \ R U H P S O R \ H H ¶ V S U R G X F W L Y L W \ R U Z R U N S H U I R U P D Q F H
x adversely affects the efficient operation of the computer system;
x results in any personal gain or profit to the user
x violates any provision of this policy, any supplemental policy adopted by the agency supplying the Internet or electronic communication systems, or any other policy, regulation, law or guideline as set forth by local, State or Federal law. (See Code of Virginia §2.1-804-805; §2.2-2827 as of October 1, 2001.)

1 R W H $ Q \ X V H U R I 9 & & 6 , 7 U H V R X U F H V H P S O R \ L Q J W K H & R P P R Q Z H D O W K ¶ V H O H F W U R Q L F F R P P X Q L F D W L R Q V V \ V W H P V I R U S H U V R Q D O X V H P X V W S U H V H Q W W K H L U F R P P X Q L F D W L R Q V L Q V X F K D Z D \ D V W R E H F O H D U W K D W W K H F R P P X Q L F D W L R Q L V S H U V R Q D O D Q G L V Q R W D F R P P X Q L F D W L R Q R I W K H D J H Q F \ R U W K H & R P P R Q Z H D O W K .

ENFORCEMENT PROCEDURE

1. Faculty, staff, students, and patrons 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.