SOUTHERN WEST VIRGINIA COMMUNITY AND TECHNICAL COLLEGE
BOARD OF GOVERNORS
SCP-7125

SUBJECT: Information Technology Acceptable Usage

REFERENCE: SCP-7720, *Security of Information Technology*; State of West Virginia Office of Technology, Information Security Policy (WVOT-PO1001, Appendix A), http://www.technology.wv.gov

ORIGINATION: July 7, 1997

EFFECTIVE: July 24, 2015

REVIEWED: September 12, 2014

SECTION 1. PURPOSE

1.1 To define and clarify the responsibilities and obligations of computer users at Southern West Virginia Community and Technical College.

SECTION 2. SCOPE AND APPLICABILITY

2.1 This issuance applies to all computer users at Southern West Virginia Community and Technical College including but not limited to guests, students, staff, faculty, and external entities.

SECTION 3. DEFINITIONS

3.1 Access – To approach or use an information resource.

3.2 Assets – Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.

3.3 Chief Information Officer – The person responsible for the agency's information resources.

3.4 Employee – For the purposes of this policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, business associates, and any other persons who are determined and notified by the Office of Information Technology (OIT) to be subject to this policy. This definition does not create any additional rights or duties.

3.5 Password – A string of characters known to a computer system or network and to a user who must enter the password in order to gain access to an information resource.

3.6 Security – Those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

3.7 User – A person authorized to access an information resource.

SECTION 4. POLICY

4.1 This policy establishes guidelines and responsibilities for users of Southern West Virginia Community and Technical College's Information Technology.

SECTION 5. BACKGROUND OR EXCLUSIONS

5.1 None.

SECTION 6. GENERAL PROVISIONS

6.1 Relevant technologies include, but are not limited to the following:

6.1.1 Personal Computers
6.1.2 Personal Digital Assistant (PDA)
6.1.3 Fax or copy machines with memory or hard drives
6.1.4 Internet or Intranet
6.1.5 E-mail and Enterprise Instant Messaging (EIM)
6.1.6 Voice Mail
6.1.7 Cell Phones (including camera phones and smart phones with data communications and databases)
6.1.8 Pagers
6.1.9 Media including disk drives, diskette drives, optical disks (CD), tape drives, and USB drives (flash drives)
6.1.10 Servers
6.1.11 Printers

6.2 Unacceptable uses include, but are not limited to the following:

6.2.1 Any use which violates local, state, or federal laws.

6.2.2 Any use for commercial purposes, product advertisements, or "for-profit" personal activity;

6.2.3 Any use for viewing, transmitting, receiving, saving, or printing sexually explicit material;

6.2.4 Any use for promotion of political or religious positions or causes;

6.2.5 Any use in relation to copyright infringement;

6.2.6 Any use in relation to participating in chain letters or unauthorized chat programs, or forwarding or responding to SPAM;

6.2.7 Any use for promoting the misuse of weapons or the use of devices associated with terrorist activities;

6.2.8 Any use related to pyramid selling schemes, multi-marketing schemes, or fund-raising for any purpose unless agency sanctioned;

6.2.9 Any use for dispersing data to customers or clients without authorization;

6.2.10 Any use in relation to placing wagers or bets;

6.2.11 Any use that could be reasonably considered as disruptive to another's work.

6.3 Users will not waste IT resources by intentionally doing one or more of the following:

6.3.1 Placing a program in an endless loop;

6.3.2 Printing unnecessary amounts of paper;

6.3.3 Disrupting the use or performance of State-provided IT resources or any other computer system or network; or

6.3.4 Storing unauthorized information or software on State-provided IT resources.

6.4 Users will not knowingly or advertently commit security violation. This includes doing one or more of the following:

6.4.1 Assessing or attempting to access records within or outside the State's computer and communications facilities for which the employee is not authorized; or bypassing State security and access control systems;

6.4.2 Copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs;

6.4.3 Violating the privacy of individual users by reading e-mail or private communications without legal authority, or authorization based upon documented just cause;

6.4.4 Misrepresenting oneself, the College, or the State of West Virginia;

6.4.5 Making statements about warranty, expressed or implied, unless it is a part of normal job duties;

6.4.6 Conducting any form of network monitoring, such as port scanning or packet filtering unless expressly authorized by the Office of Information Technology (OIT), the Vice President for Finance and Administration, or the President.

6.4.7 Transmitting through the Internet confidential data to include without limitation, credit card numbers, telephone calling cards numbers, logon passwords, and other parameters that can be used to access data without the use of encryption technology approved by the Office of Information Technology (OIT), the Vice President for Finance and Administration, or the President.

6.5 Users will not commit security violations related to e-mail activity. This includes doing one or more of the following:

6.5.1 Sending unsolicited commercial e-mail messages, including the distribution of "junk mail" or other advertising material to individuals, who did not specifically request such material;

6.5.2 Unauthorized use for forging of e-mail header information;

6.5.3 Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies;

6.5.4 Posting messages to large numbers of users (more than 50) without authorization; or

6.5.5 Posting from an agency e-mail address to newsgroups, blogs, or other locations without a disclaimer stating that the opinions expressed are strictly their own and not those of the State or the agency, unless posting is in the fulfillment of business duties.

6.6 Employee Responsibilities

6.6.1 Employees should conduct themselves as representatives of the State and College, and are responsible for becoming familiar with and abiding by all information security policies and guidelines.

6.6.2 Employees will only access files, data, and protected records if:

6.6.2.1 The employee owns the information;

6.6.2.2 The employee is authorized to receive the information; or

6.6.2.3 The information is publicly available.

6.6.3 Employees are prohibited from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, bandwidth, disk space, printer paper, or other IT resources.

6.6.4 Employees are prohibited from transmitting personal information about themselves or someone else without proper authorization while using State-provided IT resources.

6.6.5 Employees must adhere to copyright law regarding the use of software, print or electronic information, and attributions of authorship. In certain instances, legal counsel can determine permissible uses.

SECTION 7. RESPONSIBILITIES

7.1 The Chief Information Officer is responsible for administering the provisions of this policy.

7.2 Responsibilities of the User

7.2.1 Access to technology resources is a privilege Southern West Virginia Community and Technical College grants to all college faculty, staff, and students. Access may also be granted to individuals outside of the college for purposes consistent with the mission of the college, and users are responsible for complying with this policy.

7.3 Sanctions

7.3.1 Violations of the institutional purposes and policies described above are serious matters and will be dealt with as such. Violators are subject to the normal disciplinary procedures of the college and, in addition, the loss of computing privileges may result. Illegal acts involving Southern West Virginia Community and Technical College's technology resources may also be subject to prosecution by state and federal authorities.

SECTION 8. CANCELLATION

8.1 None.

SECTION 9. REVIEW STATEMENT

9.1 This policy shall be reviewed on a regular basis with a time frame for review to be determined by the President or the President's designee. Upon such review, the President or President's designee may recommend to the Board that the policy be amended or repealed.

SECTION 10. SIGNATURES

Board of Governors Chair **Date**

President **Date**

Attachments: None

Distribution: Board of Governors (12 members)
www.southernwv.edu

Revision Notes: February 2009 – This policy was revised to reflect up-to-date terms and current acceptable usage. The policy was reformatted into the new policy template.

September 2014 – This policy was revised based on the State of West Virginia Office of Technology's Information Security Policy (WVOT-PO1001) Appendix A.