SOUTHERN WEST VIRGINIA COMMUNITY AND TECHNICAL COLLEGE
BOARD OF GOVERNORS
SCP-7720

SUBJECT: Security of Information Technology

REFERENCE: State of West Virginia Office of Technology, WVOT-PO1001, Information Security Policy; WVOT-PO1006, Data Classification; http://www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx; SCP-7125, Information Technology Acceptable Usage

ORIGINATION: May 1, 1988

EFFECTIVE: July 24, 2015

REVIEWED: September 12, 2014

SECTION 1. PURPOSE

1.1 This policy establishes guidelines and responsibilities for Southern West Virginia Community and Technical College employees regarding information security and the protection of agency information resources. This information is based on the State of West Virginia Office of Technology, Information Security Policy (WVOT-PO1001) issued by the Governor's Office of Technology and is edited only to the extent necessary to clarify procedural differences between the State and the College.

SECTION 2. SCOPE AND APPLICABILITY

2.1 This policy applies to all users who have access to agency information and to systems that store, access, or process the information.

2.2 The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided information technology (IT) resources and is not necessarily all-inclusive. IT resources may include anything with a processor, communications capability, or data storage. (Please refer to SCP-7125, *Information Technology Acceptable Usage*, for a list of examples).

SECTION 3. DEFINITIONS

3.1 Access – The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.

3.2 Access Control – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

3.3 Authentication – The process of verifying the identity of a user.

3.4 Chief Information Officer (CIO) – The person responsible for the agency's information resources.

3.5 Confidential Data – Information that is legally protected (i.e., student records) or otherwise deemed by a qualified expert to be unsuitable for open access.

3.6 Contractor – Anyone who has a contract with the State or one of its entities.

3.7 Custodian of Information – The person or unit assigned to supply services associated with the data.

3.8 Employee – For the purposes of information technology and security policies, the term "employee" shall include the following: business associates, contractors, contractor's employees, subcontractors, volunteers, and individuals who are determined and notified by the institution to be subject to this policy. This definition does not create any additional rights or duties.

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

3.10 Information Resources – All information assets in all known formats.

3.11 Information 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.

3.12 Information Security Officer (ISO) – The person designated by the Chief Technology Officer to administer the agency's internal and external point of contact for all information security matters.

3.13 Information Security Incident – An event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.

3.14 Information Security Liaison (ISL) – Employees assigned by the ISO to assist in the protection of information resources.

3.15 Information Technology (IT) – The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems and applications.

3.16 Medium – Any repository, including paper, used to record, maintain, or install information or data.

3.17 Owner of Information – The person(s) ultimately responsible for an application and its data viability.

3.18 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.

3.19 Personally Identifiable Information (PII) – Includes all protected and non-protected information that identifies or can be used to identify, locate, or contact an individual.

3.20 Privacy Officer – The official responsible for facilitating the College's integration of privacy principles, legal requirements, and privacy standards into department policies, procedures, and practices.

3.21 Risk Analysis – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

3.22 Security Contact – These individuals include the Information Security Officer (ISO) and Information Security Liaison (ISL).

3.23 Threat – Includes any person, condition or circumstance that endangers the security of information, or

information systems, in the context of Information Security.

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

3.25 User ID – A unique "name" by which each user is identified to a computer system.

3.26 West Virginia Office of Technology (WVOT) – The division of the Department of Administration established by West Virginia Code § 5A-6-4a, et seq., which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

SECTION 4. POLICY

4.1 All Information Technology assets, including hardware, software, and data are owned by the College, unless accepted by contractual agreement.

4.2 Users are required to comply with legal protection granted to programs and data by copyright and license. No unauthorized software will be installed on College systems. The Office of Information Technology (OIT) will authorize all software installation.

4.3 Users will utilize, maintain, disclose, and dispose of all information resources, regardless of medium, according to law, regulation, and/or policy.

4.4 Employees must have no expectation of privacy while using State-provided information resources (i.e., cell phones, Internet, etc.).

4.5 Southern West Virginia Community and Technical College reserves the right to filter Internet site availability, and to monitor and review employee use as required for legal, audit, or legitimate authorized College operational or management purposes. By logging into their College-provided account, users are acknowledging that they have read the document and agree to follow its provisions.

4.6 All users must adhere to rules regarding unacceptable use of technology resources. (For a detailed list of unacceptable uses, see SCP-7125, *Information Technology Acceptable Usage*).

4.6.1 Users must not download, attach, change, distribute, or install any software or inappropriate files, including streaming content, for non-business functions (i.e., downloading MP3 files and/or broadcast audio or video files).

4.6.2 User must not intentionally introduce a virus into a College-provided computer, or withhold information necessary for effective virus control procedures.

4.6.3 Users must not send or share confidential information for unauthorized purposes.

4.6.4 Users must not attach or use devices on the College network that are not owned or authorized by the College.

4.6.5 Employees must not redirect confidential or privileged College data to a non-State owned computing device without proper authorization.

4.6.6 Users must not use unauthorized peer-to-peer networking or peer-to-peer file sharing.

4.6.7 Employees must never execute programs or open e-mail attachments that have not been requested or come from an unknown source. If in doubt and lacking assurance from the sender, employees should contact the Office of information Technology (OIT) Helpdesk for assistance.

4.6.8 Users must never attempt to disable, defeat, or circumvent any security firewall, proxies, web filtering programs, or other security controls.

4.6.9 Users must not use technology resources to promote harassment or illegal discrimination on the basis of race, gender, national origin, age, marital status, religion, or disability.

4.7 The Office of Information Technology (OIT), working with designated individuals, will develop procedures to protect information resources from accidental, unauthorized, or malicious access, disclosure, modification, or destruction.

4.8 Users must report any observation of attempted security or privacy violations to helpdesk@southernwv.edu.

4.8.1 A Security Incident is any event that involves misuse of computing resources or is disruptive to normal system or data processing operations. Examples include, but are not limited to the following:

4.8.1.1 Lost or stolen computers or other portable devices;

4.8.1.2 Lost or stolen media that contains sensitive data;

4.8.1.3 Rampant computer virus infections within the State network;

4.8.1.4 Loss of system or network functionality;

4.8.1.5 A disaster scenario or act of terrorism;

4.8.1.6 A prolonged power outage;

4.8.1.7 A compromised (hacked) computer or server;

4.8.1.8 A defaced Web page; and

4.8.1.9 An information security policy violation.

4.9 Users should immediately report all information security incidents to helpdesk@southernwv.edu. Users must provide the following information to the extent possible:

4.9.1 Point of contact (name, phone, e-mail);

4.9.2 Characteristics of incident;

4.9.3 Date and time incident was detected;

4.9.4 Extent of impact;

4.9.5 Nature of incident, if known (i.e., unauthorized access, system breach or malfunction, data loss or exposure, defacement, other); and

4.9.6 Any actions took in response to the incident.

4.10 Confidential, private, personally identifiable information (PII), Federal Tax Information (FTI), or other sensitive data (i.e., credit card numbers, calling card numbers, logon passwords, health information, or other protected information), must be encrypted or dissociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet.

4.11 Employees must immediately contact helpdesk@southernwv.edu upon receiving or obtaining confidential information to which the employee is not entitled or becoming aware of any inappropriate use of College-provided technology resource (Note: The owner or sender of such information must also be notified).

4.12 Employees will contact an immediate supervisor if there is doubt concerning authorization to access any College-provided technology resource, or if questions arise regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, reporting should occur up the supervisory or management chain without delay.

4.13 Access controls must be consistent with all state and federal laws and statutes, and will be implemented in accordance with this policy.

4.14 Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication.

4.14.1 All passwords are confidential and must not be shared under any circumstances.

4.14.2 Employees are expected to use strong passwords, which must conform to established standards and will be charged at intervals designated by the Office of Information Technology (OIT).

4.15 All access to computing resources will be granted on a need-to-use basis.

4.16 Individual users will be assigned unique user ID's.

4.17 Each user must be accountable for securing his or her computer, and for any actions that can be identified to have originated from it.

4.18 The Office of Information Technology (OIT) will provide network user accounts by adding, modifying, and deleting user access for customer units. Each unit will appoint a designated approval authority, who will authorize all access modifications for that unit.

4.18.1 When an employee is terminated, the unit's designated approval authority must contact the Office of Information Technology (OIT) immediately to disable all access, unless otherwise approved in writing by appropriate management.

4.18.2 When an employee transfers, the Office of Information Technology (OIT) will modify all access to accommodate new user roles and responsibilities according to instructions from the unit's designated approval authority.

4.19 All employees may be required to complete information security awareness as part of job orientation.

4.20 The authorized head of each unit must assure that all employees read this policy and understand that logging in to any system with College-provided credentials is an acknowledgment that the employee has read, fully comprehends, and will abide by College policies and procedures regarding privacy and information security.

4.21 The unit head must assure that all employees, and others who access computer systems, will receive sufficient raining in policies and procedures, security requirements, correct use of information resources, and other administrative controls.

4.22 Background checks may be conducted by the College's Human Resources department consistent with other College policies.

4.23 Data/Information Assets

4.23.1 Information resources are designated for authorized purposes. The College has a right and a duty to review questionable employee activity. Only minimal personal use of College-provided technology resources is permitted (i.e., 10-15 minutes during break and/or lunch periods). This must not include any unauthorized uses (See SCP-7125, Information Technology Acceptable Usage), and must not interfere with the legitimate business of the College.

4.23.2 All information assets must be accounted for and have assigned owners. Owners, custodians, and users of information resources must be identified and their responsibilities defined and documented.

4.23.3 Each owner or custodian of information will determine and document classification based on the circumstances and the nature of the information, according to a classification scheme common to all State agencies. Classification should consider legal protections, privacy, sensitivity, and criticality to the functions of the business. (For more information please reference WVOT-P01006, *Data Classification*).

4.23.4 The owner or custodian will determine and document the data classification, and the CIO will ensure the protective guidelines that apply for each level of information. They include, but are not limited to the following:

4.23.4.1 Access;

4.23.4.2 Use within the College;

4.23.4.3 Disclosure outside the College;

4.23.4.4 Electronic distribution; and/or

4.23.4.5 Disposal / Destruction.

4.23.5 If at any time equipment or media changes ownership or is ready for disposal, the user must alert the responsible technical staff to the potential presence of any confidential and/or sensitive data on said equipment or media.

4.24 Physical and Environmental Security

4.24.1 Information resource facilities will be physically secured by measures appropriate to their critical importance.

4.24.2 Security vulnerabilities will be determined, and controls will be established to detect and respond to threats to facilities and physical resources.

4.24.3 Employees must guard against access to files and take precautions to protect technology devices when away from the workstation. This includes but is not limited to the following:

4.24.3.1 Logging off the computer;

4.24.3.2 Locking the computer; and/or

4.24.3.3 Locking the file cabinets and drawers.

4.24.4 Critical or sensitive data handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality.

4.24.5 Equipment will be secured and protected from physical and environmental damage.

4.24.6 Equipment used outside of the College premises will be given an equal or greater degree of security protection as that of on-site information resource equipment.

4.25 Information Security Administrators

4.25.1 The CIO is assigned the role of Information Security Administrator (ISA). The ISA must perform, contract, or delegate the necessary functions and responsibilities of the position as defined in this policy and the Governor's Executive Information Security Team (GEIST) charter. If necessary, the ISA may delegate duties to one or more individuals (i.e., ISL's) whose main function will be to assist in the protection of information resources within their agency.

4.25.2 The ISA will ensure that a risk management program will be implemented and documented, and that a risk analysis will be conducted periodically.

4.25.3 The ISA will oversee and ensure that cost effective contingency response and recovery plans will be maintained, providing for prompt and effective restoration of critical business functions in the event of any disruptive incident.

4.25.4 Procedures, guidelines, and mechanisms utilized during an information security incident, along with the roles and responsibilities of the incident management teams, must be established, documented, and periodically reviewed. This may include testing to make sure that all plans remain current, viable, and comprehensive.

4.25.5 Testing will be performed at intervals designated within CTO standards.

SECTION 5. BACKGROUND OR EXCLUSIONS

5.1 None.

SECTION 6. GENERAL PROVISIONS

6.1 None.

SECTION 7. RESPONSIBILITIES

7.1 None.

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 – The policy was revised to include all forms of technology and to meet the standards of the payment card industry. The policy was reformatted using the latest policy template.

September 2014 – Extensive policy revisions were made based upon WVOT-PO1001, Information Security Policy, State of West Virginia Office of Technology.