SOUTHWEST TENNESSEE COMMUNITY COLLEGE

SUBJECT: Acceptable Usage Policy

EFFECTIVE DATE: January 21, 2010 ; Revised January 21, 2015

Purpose

This policy defines the responsible and appropriate use of the information technology resources at Southwest Tennessee Community College. This policy applies to all clients of Southwest's information technology resources, whether affiliated with the college or not, and to all clients of these resources, whether on campus or from remote locations.

Scope

Information technology resources at Southwest Tennessee Community College are available to all currently enrolled students, faculty, staff and others who have been authorized by the College for use.

Each authorized client assumes responsibility for their own behavior while utilizing these resources. While the use of computers and information technologies does not alter basic codes of behavior in academic life, it does place some issues in new contexts.

Responsible, acceptable use is always ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It is important that all users of the information technology facilities conduct their activities in this manner since they have access to many valuable and sensitive resources. One's computing practices can adversely affect the work of the College and others.

Compliance

All clients of Southwest Tennessee Community College using the College information technology resources are required to comply with this policy. Southwest reserves the right to amend this policy at any time and without prior notice in order to better provide information technology access to our clients. Southwest reserves the right to restrict or extend computing privileges and access to College technology resources.

Source of Policy: Information Technology

Responsible Administrator: Executive Director of Information Tech. Svcs

TBR Policy Reference: 1:08:00:00

Related Policy: N/A

TBR Guideline Reference: N/A

Approved: _____
President

Date: June 1, 2015

Policy

Part One General

1.1 Client Access and Privileges

1.1.1 Client Agreement

Employees and students will read and signify their acceptance of this policy upon initial login to the College network. This acceptance will be stored by client ID and date. Upon policy revision, the acceptance indicator will be issued upon the next login after posting and the last client acceptance will be recorded.

1.1.2 Client Accounts

Southwest Tennessee Community College provides appropriate access to administrative and academic information technology based on student and employee roles. Information technology services include access to administrative business systems, academic software, computer laboratories, email, telephone, Internet and intranet. This access is a privilege, not a right, and may be revoked for any reason including non-compliance with Southwest Tennessee Community College information technology policies.

1.1.2 Client ID

Employee and student clients are each responsible for any and all activity performed with their client IDs. It is the responsibility of each client to protect their ID and login information, and not share this information with others. Any suspected unauthorized use of a client ID should be reported to the Executive Director of Information Systems.

1.1.3 Passwords

Passwords are an important aspect of computer security. They are the front line of protection for our client accounts. It is the responsibility of employee and student clients to protect their passwords.

A password reset utility is available on the My.Southwest portal login page for students and employee usage.

The College Electronic Information Security Policy 4:02:20:00/37 describes the standards for the creation of strong passwords, the protection of those passwords, and the frequency of change.

1.1.4 System Privilege Termination

A. Student access will be terminated when a student has not enrolled for one year.
B. Employee access will be terminated upon separation for any reason other than emeritus status.
C. Emeritus faculty may preserve their access by request.

1.1.5 Personally Owned Computers

Southwest Tennessee Community College is not responsible for hardware, software or data kept on the personal information technology equipment of employee and student clients. The storage of Student data and/or other college privileged information on personally owned devices is prohibited.

1.2 Acceptable Use

1.2.1 Acceptable uses of Information Technology Resources

Southwest Tennessee Community College's information systems are provided to assist students and employees in acquiring and disseminating information related to the performance of classroom assignments and regularly assigned job duties.

1.2.2 Unacceptable Uses of Information Technology Resources

Any information, data, or programs not aligned with the mission of Southwest must not be created, stored or transmitted, viewed or manipulated using College owned technology or information systems.

The following is a list that includes, but is not limited to unacceptable uses of information technology or information systems.

A. Transmitting any material, or engaging in any other activity in violation of any federal, state, or local laws including copyright law.

B. Transmitting or accessing information containing harassing material. Computer harassment includes, but is not limited to:

i) Possessing text, images or audio with the intent to harass, terrify, intimidate, threaten, or offend another person.
ii) Intentionally using the computer to contact another person repeatedly with the intent to harass or bother, whether or not an actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.
iii) Intentionally using computers or other technology to disrupt or damage administrative, academic or related pursuits of another.
iv) Intentionally using the computer or other technology to invade or threaten to invade, the privacy, academic or otherwise, of another.

C. Transmitting, receiving, displaying, or viewing offensive content, which includes but is not limited to, sexual comments or images, racial slurs, gender specific comments or any comments that would offend someone on the basis of their age, sex, national origin or disability. Displaying, sending, printing, or storing sexually explicit, graphically disturbing, obscene, pornographic, fraudulent, harassing, threatening, abusive, racist or discriminatory images, files or messages in any campus facility or campus location is prohibited.

D. Disseminating or printing copyrighted materials including computer files, articles and software, in violation of copyright laws.

E. Attempting forgery of e-mail messages.

F. Authoring SPAM messages.

G. Physical or electronic interference with other computer system clients.

H. Clients may not install or use any unauthorized Peer-to-Peer (P2P) file sharing device to share or distribute:

i) Copyrighted material without authorization from the copyright owner.
ii) Privileged, private, or strategic information determined by administrators as vital to the operation of the College.
iii) Any viruses, spyware, or license keys.
iv) Software that threatens or disrupts any Southwest Tennessee Community College computing service.

Peer-to-peer file sharing programs may pose opportunities for significant loss to owners of copyrighted material and significant liability to the College. Allowing non-authorized access to computers on the College network may provide access to privileged information. Peer-to-peer programs degrade the speed of the network and they may contain spyware, viruses, or exploits that may allow unauthorized access to the computer hosting the program. These programs may provide backdoors to computer criminals with additional resources to launch attacks.

I. Any other practice or activity that, in the opinion of the College administration constitutes irresponsible behavior, promotes illegal activities, results in the misuse of computer resources or jeopardizes the operation of computer systems, available technology or network systems.

1.2.3 Commercial Use of Information Resources

Southwest technology resource clients must not use College information or technology resources for engaging in commercial activities other than those permitted by Southwest management.

1.3 Campus Computing Facilities

1.3.1 Acceptable Use of Facilities

Computer laboratories are available for open lab use when academic classes are not scheduled in them. These facilities are made available on an unmonitored basis. All clients are required to use these facilities in a responsible manner.

1.3.2 Disruptive Behavior

Clients using campus computing facilities must not cause noise, display abusive or inappropriate behavior towards other clients, or create other disturbances in any campus computing area.

1.3.3 Data Protection

Clients using campus computing facilities must not destroy or remove data other than their own.

1.3.4 Destruction of Information Technology Resources

Clients using campus computing facilities must not destroy or remove College-owned computer resources.

1.3.5 Lab Computer Configurations

Clients using the campus computing facilities must not attempt to change the set-up on lab computers.

1.3.6 Process to Report Damage

Damage to computer laboratory equipment should be reported to the Information Technology Services Department.

1.4 Privacy and Information Technology Resources

1.4.1 Legal Ownership of Information Systems Files and Messages

Southwest Tennessee Community College retains legal ownership of the contents of all files stored on its computer and network systems as well as all messages transmitted via these systems. Southwest reserves the right to access all such information without prior notice whenever there is a genuine business need to do so.

1.4.2 Responsibility for Monitoring Content of Information Systems

Southwest reserves the right to remove any message, file, database, graphic or other material from its information systems. Southwest has no obligation to monitor information content residing on or flowing thru its information systems.

1.4.3 Privacy Expectations for Internet, College Network and Files

A. At any time and without prior notice, Southwest reserves the right to examine archived electronic mail, personal file directories, hard disk drive files and other information stored on Southwest information systems.
B. At any time and without prior notice, Southwest reserves the right to examine or monitor for any reason any device attached to the College network.
C. At any time and without prior notice, Southwest reserves the right to examine or monitor the Internet usage of clients using the College network.
D. These examinations are performed to assure compliance with internal policies, to support the performance of internal investigations, to comply with legal requirements such as a subpoena or court order, and to assist with the management of Southwest's information systems. It is also possible that others may inadvertently access or monitor these same systems.

1.4.4 Disclaimer of Responsibility for Damage to Data and Programs

Southwest uses access controls and other security measures to protect confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, the College administration maintains the authority to: (1) restrict or revoke any client's privilege, (2) inspect, copy, remove, or otherwise alter any data, program or other information technology resource that may undermine these objectives, and (3) take any other steps deemed necessary to manage and protect its information systems. This authority may be exercised with or without notice to the involved users. Southwest disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

1.5 Intellectual Property

1.5.1 Copyright Laws

Clients are expected to adhere to the provisions of Public Law 96-517, Section 7(b) which amends Section 117 of Title 17 of the United States Code to allow for making of back-up copy of computer programs. The public law states that "…it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of the computer program provided:

A. A new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that is used in no other manner, or
B. A new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be within policy."

Clients are expected to adhere to the provisions of the remainder of Title 17 of the United States Code, including the limitations on the copying and distribution of musical, visual, and literary works. Works protected by copyright may not be accessed or distributed by file sharing, peer-to-peer technology, or any other method violating 17 USC 501-513.

1.5.2 Software

Respect for the intellectual work and property of others is essential to the mission of Southwest. Southwest strongly supports strict adherence to software vendor's license agreements and copyright holders' notices. It is illegal to duplicate, copy or distribute software or its documentation without the permission of the copyright owner.

If Internet users or other system clients make unauthorized copies of software, the clients are doing so on their own behalf, since all such copying is strictly prohibited by Southwest.

Only software that supports the educational and administrative mission of the College will be installed on the College's computers. That software is normally limited to:

A. Software purchased and installed under a site agreement.
B. Software purchased under a single copy purchase and installed on a single machine.
C. Software developed by employees and students.
D. Public domain software and software contributed to the college.
E. Freely available software that may not be public domain; Software licensed under GPL or BSD are examples.

Illegal copies of copyrighted computer programs may not be made or used on College equipment.

The legal or insurance protection of Southwest and the Tennessee Board of Regents will not be extended to employees or students who violate copyright laws.

Software not acquired by Southwest by an officially sanctioned means as stated above will not be installed or operated on the College computer resources.

1.5.3 Trial Licenses for Software

Freeware, shareware and trial-ware are covered by copyright and are subject to the terms and conditions defined by the holder of the copyright and copyright policies of Southwest Tennessee Community College.

1.5.4 Fair Use

Unless permission from the copyright owner(s) is first obtained, making multiple copies of materials from magazines, journals, newsletters, software documentation and other publications is prohibited unless it is both reasonable and customary. This notice of "fair use" is in keeping with international copyright laws.

1.6 Digital\Electronic Signatures and Transactions

1.6.1 Use of Digital and Electronics Signatures

Southwest Tennessee Community College must comply with the Tennessee Uniform Electronic Transactions Act (T.C.A. ?47-10-101 et seq.) This Act permits the use of electronic signatures and electronic transactions under certain circumstances.

1. In order to be legally enforceable, an electronic signature must meet the following two criteria:

A. An electronic signature must be attributable (or traceable) to a person who has the intent to sign the record or contract with the use of adequate security and authentication measures that are contained in the method of capturing the electronic transaction (e.g., use of personal identification number or personal log-in identification username and password). (T.C.A. ?47-10-109) (If Public Key Infrastructure technology ("PKI") is to be used in the creation of the digital signature, contact the Director of Information Technology who will contact the TBR Chief Information Officer prior to implementation.)

B. The recipient of the transaction must be able to print or store the electronic record of the transaction at the time of receipt. (T.C.A. ?47-10-109)

2. The use of electronic/digital signatures in compliance with state and federal laws is permitted.

Part Two Information Professionals

2.1 Handling of Third Party Confidential and Proprietary Information

Unless specified otherwise by contract all confidential or proprietary information, including software written by a third party, that has been entrusted to Southwest by a third party must be protected as though it was Southwest's confidential information.

2.2 Confidentiality of Computer Related Software or Documentation

All Southwest generated programs, codes and related documentation is confidential and must not be taken elsewhere when an employee, consultant, or contractor leaves the employ of the College.

2.3 Removal of Sensitive Information from College Premises

Confidential College information, no matter what form it is in, must not be shared with those outside Southwest or removed from the premises without following the policy regarding storage of sensitive information on portable or remote resources.

2.4 Storage of Sensitive Information on Portable or Remote Resources

Portable data devices can provide College employees easy remote data access to Southwest data storage and retrieval capabilities for business purposes. These devices include laptops, PDAs, cell phones, thumb drives and removable hard drives.

Protect any sensitive and personal identification information stored on portable data devices from unauthorized access through the use of all available measures, including, but not limited to:

A. Encryption
B. Password protection
C. Up-to-date virus protection and malicious software detection and removal products
D. Use of data destruction procedures when information is no longer needed
E. Use of procedures for purging, overwriting, or degaussing equipment when ownership changes
F. Other reasonable safeguards to prevent theft of the device and/or viewing of protected information.
G. Limit protected data and personal identification information stored on the device to the “minimum necessary” to accomplish the purpose.
H. Individuals granted extracted data receive proper training in the use of personally identifiable information thru their immediate supervisor, Information Systems or Human Resources when they are hired.

2.5 Privacy Expectations for Administrative Data

It is imperative that all administrative data is received, stored and maintained by Southwest employees in a secure and confidential manner. This information is stored in a variety of formats including hardcopy reports, electronic databases, and document imaging. Southwest is responsible for the accuracy, integrity and confidentiality of this data. Data must be treated as confidential unless designated as approved for public release. By law, certain electronic institutional data are confidential and may not be released without proper authorization to the appropriate requestor. Employees are required to be aware that their conduct

either on or off the job could affect or threaten the security and confidentiality of this information. All employees accessing administrative systems are required to adhere to the following:

A. Unauthorized use of any information in files maintained, stored or processed by any Southwest information system is prohibited.
B. No one is permitted to seek personal benefit, allow others to benefit personally or to divulge, in any way, the contents of any record or report to any person except in the conduct of his/her assignment.
C. No one shall knowingly include, or cause to be included, in any record or report, a false, inaccurate, or misleading entry. No one shall knowingly change or delete or cause to be changed or deleted an entry in any record or report, unless expressly authorized to do so and in accordance with Southwest administrative policies and procedures.
D. Information that is downloaded should not be altered in spreadsheets or word processing documents in a way that misrepresents the information derived from this data. Downloaded information should be used and represented responsibly.
E. Information that contains college privileged information should not be uploaded and stored to any third party sites, such as Dropbox, Google Docs, or similar websites. The Information Technology Services department will provide document storage options.
F. No official record or report, or copy thereof, shall be removed from the office where it is maintained or copied or printed via electronic means except in the authorized performance of a person's duties and in accordance with established procedures. Copies made for the performance of a person's duties shall not be released to third parties except when required by a work assignment.
G. Office computers as well as portable data devices such as laptops, tablets, smart phones, and other mobile devices must be locked by standard operating system lock.
H. No one is to aid, abet, or act in conspiracy with another to violate any part of these terms and conditions.
I. Any knowledge of a violation of these terms and conditions must be immediately reported to the employee's supervisor and the Executive Director of Information Technology Services or his/her designee.

Part Three Disciplinary Action

3.1 Disciplinary Action for Violation

If a College employee reasonably believes that a client is engaged in activities which may pose an imminent threat to: (1) the health or safety of others, (2) the integrity of data, (3) computing resources which may adversely affect system operations, or (4) copyrights, the employee may request the Executive Director of Information Technology Services to suspend the client's access until the issue is investigated.

Disciplinary action shall follow existing Southwest policy and procedures governed by the applicable provisions of the student handbook, faculty and staff handbooks and the applicable State and Federal laws.

The following disciplinary sanctions outline some, but are not limited to, actions that may be taken either singularly or in combination, by the Institution against violators of this policy.

A. Restitution to reimburse the College for damage to or misuse of computing facilities.
B. Warning to notify the individual that continuation or repetition of a specified conduct may be cause for other disciplinary action.
C. Reprimand in writing indicating further violation may result in more serious penalties.
D. Restriction of computing privileges for a specified period of time.
E. Probation status, with the associated implications, imposed on the individual.
F. Suspension of the individual from the College.
G. Expulsion of the individual from the College.
H. Interim or summary suspension until a final determination has been made in regard to the charges made against the individual.

In the event that other College regulations are violated, additional penalties may be imposed.

Unauthorized use of computing resources may be turned over to local law enforcement offices. This activity may be adjudged a felony and the individual (s) involved may be liable to legal prosecution.

The utilization of a hostile software program designed to do damage and interrupt normal operations of the college computer is a criminal act and, as such, punishment to the fullest extent of State and Federal law will be pursued by the College.

Part Four Meta Policy

4.1 Additions and Deletions

Suggested information policy additions, deletions or alterations must be submitted to the Executive Director of Information Technology Services, or his/her designee in order to be implemented.

4.2 Policy Review Process

This policy will be reviewed annually by the Information Technology Committee who is responsible for developing the IT plan in accordance with TBR policies and strategic goals at the College**.** Any member of this committee may request additional review by others, but policy acceptance will occur when each of the

members comprising this committee have signed in approval. Policy specifically designated for Information Professionals will be approved by the Executive Director of Information Technology Services.

4.3 Policy File

A file will be kept in the Executive Director's office maintaining this policy and the approval documents for the policy for at least 10 years.

4.4 Policy Communication

Southwest Tennessee Community College Technology policies will be available on the Information Systems web site.

4.5 Policy Summaries

Condensed versions of this policy or client-specified synopses of these policies may be distributed as needed to adequately implement the policies. Condensed versions or synopses must include information about how to obtain the complete policy or policies.