SOUTHWEST TENNESSEE COMMUNITY COLLEGE

SUBJECT: Acceptable Use of Technology Resources

EFFECTIVE DATE: January 21, 2010; Revised January 21, 2015; July 1, 2024

*In October of each year, Information Technology related policies are reviewed as required by external regulations.

I. Purpose

The purpose of this policy is to establish the responsible and appropriate use of the technology resources at Southwest Tennessee Community College ("Southwest" or "the College"), and provide measures to ensure a secure systems infrastructure, protect the confidentiality and integrity of electronic information, and ensure compliance with applicable regulations of the Tennessee Board of Regents (TBR), as well as state and federal laws.

II. Scope

This policy applies to all clients and users of Southwest's information technology resources, whether affiliated with the College or not, and to all clients and users of these resources, whether on campus or from remote locations.

Information technology resources at Southwest are available to all currently enrolled students, faculty, staff, and others who have been authorized by the College. Each authorized client or user 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, it does place some issues in new contexts.

Responsible, acceptable use is always ethical, reflects honesty, including 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. An individuals' computing practices can adversely affect the work of the College and others.

III. Compliance

All clients of Southwest 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 to better provide information technology access to clients and users. Southwest also reserves the right to restrict or extend computing privileges and access to College technology resources.

IV. General

Access and Privileges

A. Client and User Agreement – Employees and students will read and signify their acceptance of this policy upon initial login to the College's network. This acceptance will be stored by client or user ID and date. The acceptance indicator will be issued during the next login after posting, and the last client or user acceptance will be recorded.

B. Client or User Accounts – Southwest provides appropriate access to administrative and academic information technology based on student and employee roles. IT services include access to administrative business systems, academic software, computer laboratories, email, telephone, voicemail, internet, and intranet. This access is a privilege, not a right, and can be revoked for any reason including non-compliance with Southwest information technology published policies, guidelines, procedures, and practices.

C. Client or User ID – Employee and student clients and users are each responsible for the activities performed with their client or user ID. It is the responsibility of each client and user to protect their ID and login information, and not share this information with others. Any suspected unauthorized use of a client or user ID should be reported to the Chief of Administrative Services.

D. Passwords – Passwords are an important aspect of computer security. They are the front line of protection for accounts. It is the responsibility of employee and student clients and users to protect their passwords. A password reset utility is available in the my.Southwest portal login page.

   The College's Electronic Information Security Policy, 6:02:20:00/37 describes the standards for the creation of strong passwords, the protection of those passwords, and the frequency of change.

E. Two-Factor Authentication – Southwest is required by the state of Tennessee to implement a multi-factor authentication system to login and access computerized information technology resources. All faculty, staff, and students must enroll in the provided two-factor verification to access their Southwest accounts.

F. System Privilege Termination
   1. Student access will be terminated when a student has not enrolled for one (1) year.
   2. Employee access will be terminated upon separation for any reason other than emeritus status.
   3. Emeritus faculty may preserve their access upon request and with the approval of the Vice President of Academic Affairs and the Vice President of People and Culture (Human Resources). If the Vice Presidents do not agree on this matter, the President will make the determination.

G. Personally Owned Computers – Southwest is not responsible for hardware, software, or data kept on the personal information technology equipment of employee or student clients or users. The storage of student data or other privileged or confidential information on personally owned devices is prohibited.

Acceptable Use

A. Acceptable Uses of Information Technology Resources –The College's information systems are provided to assist students and employees in acquiring and disseminating information related to the performance of classroom assignments and job duties.

B. Unacceptable Uses of Information Technology Resources – Any information, data, or programs not aligned with the mission of Southwest must not be created, stored, 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:

1. Transmitting material or engaging in any other activity in violation of regulations set forth by TBR or federal, state, or local laws, including copyright law.

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

   a. Possessing text, images, or audio with the intent to harass, terrify, intimidate, threaten, or offend another person.
   b. 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 where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.
   c. Intentionally using computers or other technology to disrupt or damage administrative, academic, or related pursuits of another.
   d. Intentionally using the computer or other technology to invade or threaten to invade, the privacy, academic or otherwise, of another.

3. 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, sexual orientation, 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. See Southwest policy 3:06:00:00/24, 5:01:02:00/28, 5:00:00:00/9, 5:00:00:00/41, 5:00:00:00/15 regarding protected class and misconduct regulations.

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

5. Attempting forgery of email messages.

6. Authoring SPAM messages.

7. Physical or electronic interference with other computer system clients or users.

8. Installation or use of unauthorized peer-to-peer file sharing devices to share or distribute:

   a. Copyrighted material without authorization from the copyright owner.
   b. Privileged, private, or strategic information determined by administrators as vital to the operation of the College.
   c. Viruses, spyware, or license keys.
   d. Software that threatens or disrupts 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 can provide access to privileged information. Peer-to-peer programs degrade the speed of the network and they might contain spyware, viruses, or exploits that could allow unauthorized access to the computer hosting the program. These programs can provide backdoors to computer criminals with additional resources to launch attacks.

9. Any other practice or activity that, in the opinion of the Chief of Administrative Services, 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.

C. Commercial Use of Information Resources – Southwest technology resource clients and users must not use College information or technology resources for engaging in commercial activities other than those authorized by department heads (Vice Presidents or Chiefs).

Campus Computing Facilities

A. Acceptable Use of Facilities – Computer laboratories are available for use when academic classes are not scheduled in them. All clients and users are required to use these facilities in a responsible manner.

B. Disruptive Behavior – Individuals who use computer labs must not cause noise, display abusive or inappropriate behavior towards other clients or users, or create other disturbances.

C. Data Protection – Individuals who use computer labs must not destroy or remove data other than their own.

D. Destruction of Information Technology Resources –Individuals who use computer labs must not destroy or remove College-owned computer resources.

E. Lab Computer Configurations – Individuals who use computer labs must not attempt to change the set-up on any computer.

F. Process to Report Damage – Damage to computer lab equipment should be reported to the Information Technology Department.

Privacy and Information Technology Resources

A. Legal Ownership of Information Systems Files and Messages –The 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, as determined by the Chief of Administrative Services or the President.

B. 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. The College has no obligation to monitor information content residing on or flowing through its information systems.

C. Regarding privacy expectations for the internet, College network, and files:

1. At any time and without prior notice, the College may examine archived electronic mail, personal file directories, hard disk drive files, and other information stored on Southwest information systems.
2. At any time and without prior notice, the College may examine or monitor any device attached to the Southwest network.
3. At any time and without prior notices, the College may examine or monitor the Internet usage of clients using the Southwest network.
4. 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, to assist with the management of Southwest's information systems, and for any other purpose as determined by the Chief of Administrative Services or the President.
5. It is also possible that others may inadvertently access or monitor the information.

D. 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 communication systems. In keeping with these objectives, the College has the authority to:

1. Restrict or revoke any client or user's privilege;
2. Inspect, copy, remove, or otherwise alter any data, program, or other IT resource that may undermine these objectives; and
3. Take any other steps deemed necessary to manage and protect its information systems.

This authority can be exercised with or without notice to the involved clients or users. Southwest disclaims any responsibility or damage to data or software that results from its efforts to meet these security objectives.

Intellectual Property

A. Copyright Laws – Clients and users must adhere to the federal law as stated in 17 USC 117 and its amendments. It provides 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 that computer program provided that the new copy or adaptation is:

1. Created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner; or
2. 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 rightful.

Clients and users are expected to adhere to the remaining portions of USC Title 17, 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.

B. Software – Respect for the intellectual work and property of others is of the upmost importance. 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 may 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 usually limited to:

1. Software purchased and installed under a site agreement.
2. Software purchased under as single copy purchase and installed on a single machine.
3. Software developed by employees and students.
4. Public domain software and software contributed to the College.
5. Freely available software that may not be public domain (i.e., software licensed under GPL or BSD).

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

Neither the legal nor the insurance protection of Southwest or TBR will be extended to employees or students who violate copyright laws.

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

C. 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 the College's copyright policies.

D. Fair Use – Unless permission from the copyright owner 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.

Digital/Electronic Signatures and Transactions

A. Use of Digital and Electronic Signatures – Southwest 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.

   In order to be legally enforceable, an electronic signature must meet the following two (2) criteria:

   1. 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 login identification username and password). T.C.A. §47-10-109. (If Public Key Infrastructure technology is to be used in the creation of the digital signature, contact the Chief of Administrative Services who will consult an Information Technology representative at TBR.
   2. 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.

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

V. Information Professionals

A. 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 if it is Southwest's confidential information.

B. Confidentiality of Computer-Related Software or Documentation – All Southwest-generated programs, codes, and related documentation are confidential and must not be taken elsewhere when an employee, consultant, or contractor leaves the College.

C. 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 below regarding storage of sensitive information on portable or remote resources. This is particularly important as it relates to remote work situations. Confidential College information must be kept in the strictest of confidences without regard for an employee's work location.

D. Storage of Sensitive Information on Portable or Remote Resources – Portable data devices such as laptops, cell phones, thumb drives, and removable hard drives provide College employees with convenient access to Southwest data.

   Employees must protect 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:

   1. Encryption
   2. Password protection
   3. Up-to-date virus protection and malicious software detection and removal products
   4. Use of data destruction procedures when information is no longer needed
   5. Use of procedures for purging, overwriting, or degaussing equipment when ownership changes
   6. Other reasonable safeguards to prevent theft of the device and/or viewing of protected information
   7. Limitation of protected data and personal identification information stored on the device to the minimum necessary to accomplish the purpose
   8. For individuals who have been granted access to extracted data, proper training in the use of personally identifiable information, provided through their supervisor, Information Systems, or the Office of People and Culture (Human Resources) when they are hired.

E. Privacy Expectations for Administrative Data – It is imperative that all data is received, stored, and maintained by Southwest employees in a secure and confidential manner. 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:

   1. Unauthorized use of information in files maintained, stored, or processed by any Southwest information system is prohibited.
   2. No one may seek personal benefit or allow others to personally benefit from the contents of any record or report. The contents of records and reports are only to be divulged at the direction of an employee's supervisor.
   3. No one shall knowingly include, or cause to be included, in any record or report, a false, inaccurate, or misleading entry.
   4. 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 policies and procedures.

5. Information that is downloaded should not be altered in a way that misrepresents the information derived from this data. Downloaded information should be used and represented responsibly.
6. Content that contains Southwest's privileged information should not be uploaded and stored to any third-party sites, such as Dropbox, Google Docs, or similar websites. The Information Technology Department can provide document storage options.
7. 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.
8. Office computers as well as portable data devices (such as laptops, tablets, and telephones) must be locked by standard operating system lock.
9. No one is to aid, abet, or act in conspiracy with another to violate any part of this policy.
10. Any knowledge of a violation of these terms and conditions must be immediately reported to the employee's supervisor and the Chief of Administrative Services.

VI. Disciplinary Action

A. Disciplinary Action for Violation – If a College employee reasonably believes that a client or user is engaged in activities that might pose an imminent threat to: (1) the health or safety of others; (2) the integrity of data; (3) computing resources that might adversely affect system operations; or (4) copyrights, the employee must advise the Chief of Administrative Services, who will determine whether to suspend the client or user'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 College against violators of this policy.

1. Restitutions to reimburse the College for damage to or misuse of computing facilities.
2. Warning to notify the individual that continuation or repetition of a specified conduct may be cause for other disciplinary action.
3. Reprimand in writing indicating further violation may result in more serious penalties.
4. Restriction of computing privileges for a specified period of time.
5. Probation status, with the associated implications, imposed on the individual.
6. Suspension of the individual from the College.
7. Expulsion of the individual from the College.
8. 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.

VII. Meta Policy

A. Additions and Deletions – Suggested information, policy additions, deletions, or alterations must be submitted to the Chief of Administrative Services, or designee, in order to be implemented.

B. Policy Review Process – This policy will be reviewed annually by the Chief of Administrative Services, who is responsible for developing the IT plan in accordance with TBR policies and strategic goals at the College. Policies specifically designated for Information Professionals will also be approved by the Chief of Administrative Services.

C. Policy File – A file will be kept in the Chief of Administrative Services' office maintaining this policy and the approval documents for at least ten (10) years.

D. Policy Communication – Southwest's technology policies will be available in the College's virtual Policy Manual found on the College's website.

E. Policy Summaries – Condensed versions of this policy or client/user-specified synopses may be distributed as needed to adequately implement. Condensed versions or synopses must include information about how to obtain the complete policy.

Source of Policy: Business and Finance

Responsible Administrator: Chief of Administrative Services

Related Policy: 6:00:00:00/15; 6:02:20:00/37

TBR Policy Reference: 1.08.00.00

Approved: Tracy D. Hall
President

Date: July 1, 2024