AIKEN TECHNICAL COLLEGE
PROCEDURE

Procedure Title:	ACCEPTABLE USE	Procedure Number:	2-7-101.10
Institutional Authority:	Chief Business Officer		
Associated SBTCE Policy/Procedure:			
Governing ATC Policy:	2-7-101		

Approved: _____ _____
President Chief Business Officer

Date Adopted: 11/18/2019
Date Revised: 12/13/2021

DISCLAIMER

PURSUANT TO SECTION 41-1-110 OF THE CODE OF LAWS OF SC, AS AMENDED, THE LANGUAGE USED IN THIS DOCUMENT DOES NOT CREATE AN EMPLOYMENT CONTRACT BETWEEN THE EMPLOYEE AND THE AGENCY.

Information is considered to be an asset of Aiken Technical College. For purposes of this procedure, information is intended to be broadly defined and is understood to mean all information, regardless of the form or format, which is created, acquired, or used in support of the activities of Aiken Technical College.

Access to computer systems, electronic devices, and networks owned or operated by the State of South Carolina imposes certain responsibilities and obligations on state employees and public officials (herein termed users) and is subject to State Government policies and local, state, and federal laws. Acceptable use of the aforementioned is always ethical, reflects honesty, and shows restraint in the consumption of shared resources at all times. Acceptable use demonstrates respect for intellectual property, ownership of information, system security mechanisms, and freedom from intimidation, harassment, and unwarranted annoyance.

I. System Usage

A. Reasonable Personal Use of Computer and Communications Systems – College Information Technology (IT) resources are for college business use. This does not preclude incidental use of resources provided that they are limited and do not interfere with business activities or IT resources availability. Aiken Technical

College allows computer users to make reasonable personal use of its electronic mail and other computer and communications systems. All such personal use must be consistent with conventional standards of ethical and polite conduct. For example, electronic mail must not be used to distribute or display messages or graphics which may be considered by some to be disruptive or offensive (such as sexual jokes or pornography).

B. Use at Your Own Risk - Users access the Internet with Aiken Technical College facilities at their own risk. Aiken Technical College is not responsible for material viewed, downloaded, or received by users through the Internet. Electronic mail systems may deliver unsolicited messages that contain offensive content.

C. Activity Monitoring - Users must be aware that their Internet activity while using Aiken Technical College systems or personally owned devices on the College's network may be monitored and recorded. This information may include websites visited, files downloaded, time spent on the Internet, and related information.

D. Compliance Audit - All devices on Aiken Technical College Networks, including personally owned devices, may be audited to ensure that each device complies with Aiken Technical College policies.

E. Device Quarantine - All devices on Aiken Technical College networks, including personally owned devices, found to be out of compliance with Aiken Technical College policies may be quarantined from the network until all deviations are corrected and validated by the Information Systems Management department.

F. Unattended Active Sessions - Users must not leave their personal computer (PC), workstation, or terminal unattended without logging out or invoking a password-protected screen saver.

G. Session Timeout - Users must set the time frame for this period of no activity, at which point the contents of the screen are obscured. If sensitive information resides on a PC, the screen must immediately be protected with this access control package, or the machine turned off, whenever a user leaves the location where the PC is in use.

II. User IDs and Passwords

A. Personal User IDs Responsibility - Users must be responsible for all activity performed with their personal user IDs. They must not permit others to perform any activity with their user IDs, and they must not perform any activity with IDs belonging to other users.

B. Access Code Sharing Prohibited - Aiken Technical College computer accounts, user IDs, network passwords, voice mailbox, personal identification numbers, credit card numbers, and other access codes must not be used by anyone other than the person to whom they were originally issued.

C. Sharing Passwords - Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. Information Systems Management Department staff must never ask users to reveal their passwords.

D. Strong Passwords - Users must choose passwords that are difficult to guess. For example, users must not choose a dictionary word, derivatives of user IDs, common character sequences, details of their personal history, a common name, or a word that reflects work activities.

E. Typing Passwords When Others Are Watching - Users must never type their passwords at a keyboard or a telephone keypad if others are known to be watching their actions. To do so unduly exposes the information accessed thereby to unauthorized access.

F. Password Proximity to Access Devices - Users must never write down or otherwise record a readable password and store it near the access device to which it pertains.

G. Passwords in Communications Software – Users must not store fixed passwords in Internet browsers, or related data communications software at any time.

H. Suspected Password Disclosure - Each user must immediately change his or her password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

III. Electronic Messaging

A. Identity Misrepresentation - Users must not misrepresent, obscure, suppress, or replace their own or another person's identity on any Aiken Technical College electronic communications.

B. Handling Attachments - All electronic mail attachment files from third parties must be scanned with an authorized virus detection software package before opening or execution.

C. No Guarantee of Message Privacy - Aiken Technical College cannot guarantee that electronic communications will be private. Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users must accordingly be careful

about the topics covered in Aiken Technical College electronic communications, and should not send a message discussing anything that they would not be comfortable sharing publicly.

D. Responding to Personal Information Requests - Aiken Technical College users must never respond to electronic mail messages that request personal or sensitive company information, even from internal sources. The Aiken Technical College Information Systems Management department will never request that you perform security duties, such as changing your password, via electronic mail. Any such requests will be confirmed with separate communication from management.

E. Responding to Offensive Messages - Users must not respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications but instead report these instances to the Information Systems Management department.

F. Harassing or Offensive Materials - Aiken Technical College computer and communications systems are not intended to be used for, and must not be used for the exercise of the user's right to free speech. These systems must not be used as an open forum to discuss Aiken Technical College organizational changes or business policy matters. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Users must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others.

G. Message Forwarding - Aiken Technical College's confidential information must not be forwarded to any party outside Aiken Technical College without prior approval from the originator of the information. Messages sent must not be forwarded unless the sender clearly intended this and such forwarding is necessary to accomplish a customary business objective. In all other cases, forwarding of messages sent by outsiders to other third parties can be done only if the sender expressly agrees to this forwarding.

H. Secret Data Transmission - All Aiken Technical College sensitive data transmitted over any communication network must be encrypted and employ an approved two-factor authentication (2FA) technology.

IV. Internet Web Usage

A. Posting Sensitive Information - Users must not post unencrypted sensitive Aiken Technical College material on any publicly accessible computer that supports anonymous File Transfer Protocol (FTP) or similar publicly accessible services.

B. Disclosing Internal Information - Users must not publicly disclose sensitive internal Aiken Technical College information by posting to any website, including blogs, newsgroups, chat groups, or social networking sites. Such information includes business prospects, products now in research and development, product performance analyses, product release dates, and internal information systems problems. Responses to specific customer electronic mail messages are exempted from this policy.

C. Offensive Websites - Aiken Technical College is not responsible for the content that users may encounter when they use the Internet. When and if users make a connection with websites containing objectionable content, they must promptly move to another site or terminate their session. Users using Aiken Technical College computers who discover they have connected with a website that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site.

D. Blocking Sites - The ability to connect with a specific website does not in itself imply that users of Aiken Technical College systems are permitted to visit that site. Aiken Technical College may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation. These file types include, but are not limited to, graphic and music files.

V. Data Storage

A. Establishing Third-Party Networks - Users must not establish any third-party information storage network that will handle sensitive or restricted Aiken Technical College information (electronic bulletin boards, blogs, cloud storage) without the specific approval of the Information Systems Management department.

VI. Internal Systems

A. Eradicating Computer Viruses - Any user who suspects infection by a virus or malicious software must immediately call the Technology help desk, and make no attempt to eradicate the virus themselves without help from the Information Systems Management department.

B. Trusted Software Scanning - Users must not use any externally-provided software from a person or organization other than a known and trusted supplier unless the software has been scanned for malicious code and approved by the Information Systems Management department.

C. Prohibition Against All Forms of Adult Content - All forms of adult content (pornography or what some would consider to be pornography) are prohibited on

Aiken Technical College computers and networks. This includes content obtained via websites, email attachments, CD-ROMs, and file sharing networks.

D. Unauthorized Software and Data Copies - Aiken Technical College strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If Internet users or other system users make unauthorized copies of software, the users are doing so on their own behalf, since all such copying is strictly forbidden by Aiken Technical College. Likewise, Aiken Technical College allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.

E. Involvement with Computer Viruses - Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any Aiken Technical College computer or network.

F. External Storage Checking - Externally-supplied CD-ROMs, and other removable storage media must not be used unless they have been checked for viruses.

VII. Personal Equipment

A. Current Virus Software - Every Aiken Technical College user who examines, processes, or stores Aiken Technical College information using a computer that he or she owns must install and regularly run the most current version of a virus detection software package.

B. User Installation of Software - Users must not install software on their college-issued computers, network servers, or other machines without receiving advance authorization to do so from the Information Systems Management department.

C. Unattended Active Sessions - If the computer system to which they are connected or which they are using contains sensitive information, users must not leave their PC, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.

D. Accepting Security Assistance from Outsiders - Users must not accept any form of assistance to improve the security of their computers without first having the provider of this assistance approved by the Information Systems Management department. This means that users must not accept offers of free consulting services, must not download free security software via the Internet, and must not employ free security posture evaluation web pages, unless the specific provider of the assistance has been previously approved.

VIII. Physical Security

A. Positioning Display Screens - The display screens for all PCs used to handle sensitive or valuable data must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas. Care must also be taken to position keyboards so that unauthorized persons cannot readily see users enter passwords, encryption keys, and other security-related parameters.

B. Locking Sensitive Information - When not being used by authorized users, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other secure locations. When not being used, or when not in a clearly visible and attended area, all computer storage media containing sensitive information must be locked in similar enclosures.

C. Custodians for Equipment - The primary user of a PC is considered a custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a custodian must promptly inform the Information System Management department. With the exception of portable machines, PC equipment must not be moved or relocated without the knowledge and approval of the involved Information System Management department.

D. Use of Personal Equipment - Users must not bring their own computers, computer peripherals, network devices, or computer software into Aiken Technical College facilities without prior authorization from their supervisor. Users must not use their own PCs for Aiken Technical College business unless these systems have been evaluated and approved by the Information Systems Management department.

E. Property Pass - College-issued computers and related information systems equipment must not leave Aiken Technical College offices unless properly authorized.

IX. Telephones and Voice Mail

A. Sensitive Information On Voicemail - Users must not record messages containing sensitive client information on answering machines or voicemail systems.

B. Use of VoIP on PCs - Aiken Technical College users must not make college-supported telephone calls that communicate confidential or secret information using softphones that support voice over IP on their PCs, unless encrypted and secured.

X. Security Incident Reporting

A. Reporting Security Events - Any suspected events that may compromise information security or are known to violate an existing security policy must be immediately reported to the Information Security Manager. Examples of these events include:

- Any unauthorized use of Aiken Technical College information systems;
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed;
- All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages;
- Suspected or actual disclosure of sensitive Aiken Technical College information to unauthorized third parties.

XI. Violations

A. Any violation of this policy may result in disciplinary action, up to and including termination of employment. Aiken Technical College reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Aiken Technical College does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Aiken Technical College reserves the right not to defend or pay any damages awarded against employees or partners that result from a violation of this policy.

B. Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her supervisor or the Human Resources department as soon as possible.