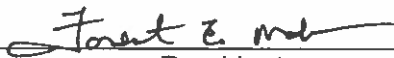


**AIKEN TECHNICAL COLLEGE
PROCEDURE**

Procedure Title:	ACCESS CONTROL	Procedure Number:	2-7-101.3
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.

This procedure defines the requirements for secure access to Aiken Technical College information and communications systems.

I. Access Restrictions

- A. Authorized Use - Aiken Technical College shall ensure that only authorized individuals have access to Aiken Technical College data/information and that such access is strictly controlled, and audited in accordance with the concepts of "need-to-know, least-privilege, and separation of duties".
- B. Least Privilege Access – Aiken Technical College shall implement processes or mechanisms to:
- Disable file system access not explicitly required for system, application, and administrator responsibilities;
 - Provide minimal physical and system access to contractors and ensure information security policy adherence by all contractors;
 - Restrict use of database management to authorized database administrators;

- Grant access to authorized users based on their required job duties.
- C. Access Control - With the exception of guest resources, all Aiken Technical College technology platforms (i.e. network, operating system, application, and database) must authenticate the identity of users (including other systems accessing these platforms) using unique user IDs and passwords and establish conditions for group membership.
 - D. Multi-Factor Authentication - Aiken Technical College shall implement a suitable multifactor authentication technique to substantiate the claimed identity of a user for Virtual Private Network (VPN) remote access connections to specific college assets identified by Information Systems Management.
 - E. Unique User ID and Password Required - Every user must have a unique user ID and a personal password, along with specified access rights for access to Aiken Technical College computers and computer networks. Shared or group user IDs must not be created or used unless necessary for operational reasons; group IDs shall be formally approved and documented by Information Systems Management.
 - F. Obfuscation - Aiken Technical College shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
 - G. Encryption – Aiken Technical College shall implement encryption as an access control mechanism if required by Federal, State, or other laws or regulations.
 - H. User Accountability - Users are accountable for all activity associated with their User ID and password. Users must never share their personal login credentials with any other person.

II. User ID and Account Management

- A. User ID Construction- All user IDs on Aiken Technical College computers and networks must be constructed according to the Aiken Technical College user ID construction standard.
- B. Default Accounts - Default user accounts on servers shall be removed or disabled and, if user accounts cannot be removed or disabled, they should be renamed.
- C. Reuse of User IDs - Each Aiken Technical College computer and communication system user ID must be unique, connected solely with the user to whom it was assigned, and must not be reassigned after a user or customer terminates their relationship with Aiken Technical College.

- D. Account Auditing – Aiken Technical College shall implement mechanisms to record successful and failed authentication attempts. All inactive accounts associated permissions must also be audited periodically.

III. Access Authorization

- A. Access Control Authorization Form - Requests for the addition, deletion, and modification of all user IDs, credentials, and other identifier objects on Aiken Technical College computer and communications systems must be submitted and authorized by the user's immediate supervisor, manager, or data owner.
- B. Logical Access - Aiken Technical College shall enforce approved authorizations for logical access to information systems.
- C. User Requests - Access requests from users shall be recorded and follow the Aiken Technical College established approval process. All user access requests must be approved by a data owner for any role not pre-approved.
- D. Evidence of User Agreement - Before they are granted access to Aiken Technical College networks and information systems, all users must provide documented evidence of their agreement to comply with Aiken Technical College authentication policies, including the Aiken Technical College policy to keep passwords confidential and to keep group passwords (shared user names for multiuse software/hardware applications) solely within the members of the group.
- E. Third-Parties – Aiken Technical College shall define security requirements for contractors, vendors, and other service providers.

IV. Account Maintenance and Review

- A. Inactive Account Maintenance - All accounts must be either removed or disabled after a specified number of days of inactivity.
- B. Account Deactivation – Aiken Technical College shall establish a process to notify relevant personnel (e.g., account managers, system administrators) to remove or deactivate access rights when users are terminated, transferred, or access rights requirements change.
- C. Guest and Temporary Accounts – Aiken Technical College shall authorize and monitor the use of guest/anonymous and temporary accounts, and notify relevant personnel (e.g., account managers) when temporary accounts are no longer required.

- D. User Access Review – Aiken Technical College shall implement processes to enforce periodic user access reviews (e.g., semi-annual) to be performed by information/data owners or their assigned delegate(s) to ensure the following:
- Access levels remain appropriate, based upon approvals;
 - Terminated employees do not have active accounts;
 - There are no group accounts, unless approved; and
 - There are no duplicate user identifiers.

V. Administrator and Privileged Accounts

- A. Administrative and Privileged Account Approval - Whenever user IDs, business application system privileges, or system privileges involve capabilities that go beyond those routinely granted to general users, they must be approved in advance by the user's immediate supervisor, the Information Owner, and the Information Systems Management department.
- B. Privilege Restriction — Need to Know - The computer and communications system privileges of all users, systems, and programs must be restricted based on the need to know principles and in accordance with a role-based access model. Access not explicitly permitted shall be denied by default.
- C. Privileged Account Review - Privileged accounts must be controlled, monitored, and can be reported on a periodic basis.
- D. Information System Accounts – Aiken Technical College shall review information system accounts within every one-hundred eighty (180) days.
- E. Separation of Duties Controls – Aiken Technical College shall implement controls in information systems to enforce separation of duties through assigned access authorizations, including but not limited to:
- Divide critical business and information system management responsibilities;
 - Divide information system testing and production functions between different individuals or groups; and
 - Independent entity to conduct information security testing of information systems.
- F. Systems Administrator User IDs - System administrators managing computer systems with more than one user must have at least two user IDs, one that provides privileged access and is logged, and the other that provides the privileges of a normal user for day-to-day work.

VI. Password Requirements & Administration

- A. Password Change Requirements - All users must be automatically required to change their passwords at least once every 180 days.
- B. Systems Administrator Passwords - Automatically force system administrators (including database, network, and application administrators) to change user account passwords no less than every 90 days.
- C. Service Accounts - Passwords for service accounts will be changed as necessary.
- D. Password Complexity - Passwords shall be created with the following requirements:
 - All passwords must have at least 8 alphanumeric characters (i.e., upper- and lowercase letters, and numbers) and/or special characters;
 - The use of dictionary names or common words based on personal information as passwords are prohibited;
- E. Password History – Passwords shall be prohibited from reuse.
- F. Password Sharing - Aiken Technical College users shall not share passwords with others under any circumstance.
- G. System Passwords - System passwords shall be changed immediately upon separation of employment of any employee with privileged access.
- H. Compromised Passwords - Aiken Technical College shall implement a process to change passwords immediately if there is reason to believe a password has been compromised or disclosed to someone other than the authorized user.
- I. User Verification - Aiken Technical College shall establish a process to verify the identity of a user prior to providing a new, replacement, or temporary password.
- J. Non-Aiken Technical College Users - Aiken Technical College shall establish a process to uniquely identify and authenticate non-Agency users.
- K. First-time Passwords - First-time passwords shall be set to a unique value per user and changed immediately upon the next login.
- L. Temporary Passwords - Aiken Technical College shall provide temporary passwords to users in a secure manner; the use of third parties or unprotected (i.e., clear text) electronic mail messages shall be prohibited.

- M. Default Passwords – Aiken Technical College shall not allow default passwords for network and remote applications.
- N. Null Passwords Always Prohibited - At no time, may any Systems Administrator or Security Administrator enable any user ID that permits password length to be zero (a null or blank password).

VII. Session Controls

- A. Session Timeout – Access control systems must be configured to automatically lock or log off users after a specified period of inactivity.
- B. Maximum Logon Attempts – Access control systems must be configured to automatically disable User IDs after an Aiken Technical College defined number of unsuccessful logon attempts. The User ID must be automatically locked after meeting this threshold.
- C. Account Lockout Duration – All user IDs that have been locked out or disabled must remain locked for a period of time commensurate with the classification of data hosted, processed, or transferred by the information system.
- D. Incorrect Logon Information - When logging on to an Aiken Technical College computer or data communications system, if any part of the logon sequence is incorrect, the system must terminate the session and wait for the correct logon information

VIII. Emergency Access

- A. Emergency Procedures - Aiken Technical College shall establish processes and procedures for users to obtain access to required information systems on an emergency basis. The emergency procedures shall ensure that:
 - Only identified and authorized personnel are allowed access to live systems and data;
 - All emergency actions are documented in detail; and
 - Emergency action is reported to management and reviewed in an orderly manner.

IX. Remote Access Security Documentation and Process

- A. Remote Access Processes – Procedures for authorized individuals to access information systems from external systems shall be developed.

- B. Remote Access Assessments - Audits or assessments must be performed periodically to ensure that the Aiken Technical College remote access policies, processes, and procedures are being followed.

X. Data Integrity

- A. Sensitive Data Transmission - All Aiken Technical College sensitive data transmitted over any communication network must be encrypted.
- B. Standard Encryption Algorithm and Implementation - If encryption is used, government-approved standard algorithms and standard implementations must be consistently employed.
- C. Transportable Computers with Sensitive Information - All portables, laptops, notebooks, and other transportable computers containing sensitive Aiken Technical College information must consistently employ hard disk encryption for all files.
- D. Remote Device Encryption Keys - The creation and use of cryptographic keys for encrypting data stored on remote devices must follow the same Aiken Technical College policies for encrypting data stored on non-remote systems.

XI. Server and Device Management

- A. Remote Access Server and Device Security - All Aiken Technical College remote access servers and devices must be kept fully patched, operated using an organization-defined security configuration baseline with approved protocols, and only managed from a limited number of trusted hosts by authorized administrators.
- B. Remote Administration - Remote administration of Internet-connected computers must be performed only over encrypted links.
- C. Remote Access Device Management Training - All Aiken Technical College employees who are responsible for the management of any remote access devices must be trained to properly secure these devices.
- D. Remote Server and Device Disposal – All sensitive information must be removed from any remote server or device prior to its disposal.

XII. Network Security Management – Diagrams

- A. Network Diagram - A network diagram that illustrates all connections to components that process or store confidential information (including any wireless networks) must be developed and maintained.

- B. External Network Connection Inventory - The Information Systems Management Department must maintain a current inventory of all connections to external networks including, but not limited to, telephone networks, EDI networks, Internet trading partner networks, wireless networks, extranets, and the Internet.

XIII. System Configuration

- A. Public Internet Servers - Public Internet servers must be placed on subnets, separate from internal Aiken Technical College networks, and to which public traffic is restricted by routers or firewalls.
- B. Systems Interfacing External Networks - All Aiken Technical College systems interfacing external networks must be running supported and updated versions of the vendor-supplied operating system software.
- C. Shared Directory Systems - The use of shared directory systems on any Aiken Technical College computer that is Internet connected or directly reachable through the Internet must be approved by Information Systems Management.
- D. External Network Interfaces - Aiken Technical College systems designers and developers must restrict their usage of external network interfaces and protocols to those that have been expressly approved by Information Systems Management.

XIV. Third Party Network Access

- A. Network Connections with Outside Organizations - The establishment of a direct connection between Aiken Technical College systems and computers at external organizations, through the Internet or any other public network, must be approved by Information Systems Management.

XV. Firewalls and Traffic Control

- A. Internet Access - All Internet access using computers in Aiken Technical College offices must be routed through a firewall or similar device that will provide firewall functionality.

XVI. Network Segregation

- A. Network Traffic Restriction - All inbound and outbound traffic must be restricted to that which is necessary for the Aiken Technical College data environment.
- B. Network Protocol Restriction - All inbound and outbound traffic must be protected by a Demilitarized Zone (DMZ) that permits only the protocols that are necessary for the Aiken Technical College data environment.

- C. Inbound Internet Traffic Limitation - Inbound Internet traffic must be limited to IP addresses within the DMZ unless approved by the Information Systems Management leadership team.
- D. Internal Address Limitation - The Aiken Technical College network must be configured such that no internal addresses are permitted to pass from the Internet into the DMZ.
- E. Database Segregation - Any database that contains confidential Aiken Technical College information must be placed in an internal network zone, segregated from the DMZ.

XVII. Phones and PBX

- A. Communication Line Changes - Users and vendors must not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not obtained approval from Information Systems Management.

XVIII. Domain Management

- A. Internet Domain Name Registration - Payments and paperwork for Internet domain name registrations for all of Aiken Technical College's official sites must be handled in a timely manner and promptly confirmed by Information Systems Management.

XIX. Firewall Security Management Implementation

- A. External Connections - All in-bound real-time Internet connections to Aiken Technical College internal networks or multi-user computer systems must pass through a firewall before users are allowed to logon. Aiken Technical College computer system may be attached to the Internet only when protected by a firewall.
- B. Virtual Private Networks - All inbound traffic, with the exception of Internet mail, approved news services, and push broadcasts, that accesses Aiken Technical College networks must be encrypted with an Information Systems Management approved VPN product.
- C. Secured Subnets - Portions of the Aiken Technical College internal network that contain sensitive or valuable information must employ a secured subnet. Access to this and other subnets must be restricted with firewalls and other access control measures. Based on periodic risk assessments, the Information Systems Management department will define the secured subnets required in the Information Systems Architecture.

- D. Demilitarized Zones – All Internet commerce servers including payment servers, and web servers must be protected by firewalls, and be located within a DMZ.
- E. Network Address Protection - Network Address Translation (NAT) is the preferred method for protecting internal IP addresses. Configuration and operation standards are implemented and maintained to preclude internal business information from being resident on or processed by any firewall, server, or other computer that is shared with another organization at an outsourcing facility. (Shared routers, hubs, modems, and other network components provided by an outsourcing organization are permissible.)
- F. Default to Denial - Every connectivity path and service not specifically permitted by this standard and supporting documents issued by Information Systems Management is blocked by default by Aiken Technical College firewalls.
- G. Firewall Access Privileges - Privileges to modify the functionality, connectivity, and services supported by firewalls is restricted to the Firewall Administrators.
- H. Firewall Physical Security - All Aiken Technical College firewalls must be located in locked rooms, closets, or cabinets that meet Aiken Technical College Physical Security standards and which are accessible only to Information Systems Management personnel and to Aiken Technical College Physical Security.

XX. Firewall Operation

- A. Monitoring Vulnerabilities – Firewall Administrators are expected to subscribe to the best internet alert advisories available and other relevant sources providing current information about firewall vulnerabilities. Any vulnerability that appears to affect Aiken Technical College networks and systems must promptly be brought to the attention of the Information Systems Management (ISM) leadership team.
- B. Intrusion Detection\Intrusion Prevention – All firewalls must include at least one or more of the standard intrusion detection and or intrusion prevention methods\systems specified by the firewall vendor. Each of these intrusion detection\protection systems is to be configured according to the specifications defined by Information Systems Management.
- C. Event Notification - Alarms from these intrusion detection\prevention systems are configured to immediately notify by cell phone or other mobile device, the technical staff that is on-call to take corrective action.
- D. Firewall Logs – All firewalls must be configured to log events according to the following standards for logging firewall activity include:

- All changes to firewall configuration parameters, enabled services, and permitted connectivity paths.
- All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures.
- Periodic log review to ensure the secure operation of the firewalls.

XXI. Change Management

- A. Posting Updates - All Aiken Technical College-approved firewalls subscribe to software maintenance and software update services.
- B. Production Firewall Change Management – Because firewalls are critical production systems, all changes to the firewall software and or hardware provided by vendors -- excluding vendor-provided upgrades, patches, and fixes – are processed for review and approval by the ISM leadership team. Major changes to the internal networking environment, any changes to the production business applications supported, and any major information security incident triggers an additional and immediate review of the firewall policy.
- C. Firewall Rule (aka “Policy”) Change Management Process – All changes to a firewall rule-set (aka “policy”) require the following process over and above the standard Change Management process:
 - 1) Require 24-hour lead time for all firewall rule change requests.
 - 2) All firewall rule change requests must include the following pieces of information:
 - a) Source address(es), including IPs and domain names (where applicable)
 - b) Destination address(es), including IPs and domain names (where applicable)
 - c) Port(s) or application requested to be open
 - d) Date when the change should be made
 - e) Point of contact
 - f) Department name
 - 3) All firewall rule change requests will be evaluated to ensure that they conform to current security best practices and current Aiken Technical College security policy.
 - 4) Emergency firewall rule change requests must be approved by a minimum of two members of the ISM leadership team.

XXII. Remote Access Management Required Approval

Remote Working Privileges - Working at home or alternative site work arrangements, both known as remote working, are a management option, not a

universal employee fringe benefit. Telecommuting must be approved in accordance with SBCTCE 8-7-106.1 Procedure, Telecommuting.

XXIII. Wireless Security Management – Installing & Configuring A Wireless Network

- A. Access Restrictions - Aiken Technical College shall establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
- B. System Hardening - Aiken Technical College shall authorize wireless access to information systems prior to allowing the use of wireless networks.
- C. Approved Personnel Only - All wireless access points must be installed by and configured by an authorized member of Information Systems Management or authorized contractors.

XXIV. Automatic Discovery of Wireless Networks

- A. Automatic Discovery - To enforce this policy, Information Systems Management will use automated means to detect the presence of all internal-network-connected devices and take steps to disable and remove such devices.
- B. Unauthorized Wireless Access Points - If an unauthorized wireless access point is detected on the Aiken Technical College network, Information Systems Management leadership must be notified.
- C. Procurement of wireless technology - Users must not purchase, rent, or otherwise procure wireless equipment on their own. These procurements of hardware, software, and services related to wireless networks must be channeled through the Procurement department. This process helps to ensure that these purchases are consistent with existing internal technical standards and security requirements.

XXV. Logical and Physical Security of Wireless Access Points

- A. User Authentication - Aiken Technical College shall use wireless networking technology that enforces user authentication to gain access to networking resources.
- B. Logical and Physical Separation - All wireless access points must be logically distinguished from, and walled off from the main internal Aiken Technical College internal network using configurations approved by Information Systems Management.

- C. Encryption and Intrusion Controls - Aiken Technical College wireless network access points must always be configured so that they consistently employ communications encryption, firewalls, and other security measures defined by Information Systems Management.

XXVI. Cloud Computing – Cloud Approval and Governance

- A. Approval Required - Use of cloud computing services for Aiken Technical College business purposes must be formally authorized by Information Systems Management. Employees must not open cloud service accounts or enter into cloud service contracts for the storage, manipulation, or exchange of company-related communications or company-owned data without prior approval from the ISM leadership team.
- B. Vendor Validation – All third-party processing (cloud) vendors must be approved by Information Systems Management.
- C. Control Compliance – Additional control requirements adopted as part of cloud arrangements must be formally adopted into the Aiken Technical College internal control framework.

XXVII. Access Controls

- A. Access Credentials - Employees and contractors establishing login credentials at third-party (cloud) services must comply with existing Aiken Technical College security requirements for secure passwords.
- B. Password Sharing – Employees and contractors establishing login credentials at third-party (cloud) services must not use the same passwords as those for local accounts.

XXVIII. Privacy Controls

- A. Foreign Data Transfer – Customer Personally Identifiable Information (PII) must not be stored in third-party (cloud) environments that are located in foreign countries.

XXIX. Sensitive Data Storage

- A. Personal Data Storage - Personal cloud services accounts may not be used for the storage, manipulation or exchange of college-related communications or college-owned data.