**Revision Responsibility:** Associate Vice President, Information Technology
**Responsible Executive Officer:** Vice President, Finance and Administration

**Source/Reference:**

## PURPOSE

I. Personally owned computing devices are increasingly being used to access College technology resources and data. A security breach when using a personal device could result in loss or compromise of College data, damage and/or unauthorized access to College technology resources, and/or financial harm to the College.

II. The purpose of this policy is to establish minimum security requirements for personally owned devices which connect to College technology resources and/or access College data. This policy does not apply to College-owned devices. For more information regarding College-owned devices, refer to the Acceptable Use Policy 07:04:01.

## SCOPE

This policy applies to all employees, contractors, students, and any other individuals who are authorized to use Columbia State technology resources.

## DEFINITIONS

A. Authentication means verifying the identity of a user, process, or device to allow access to a College technology resource.

B. College data means anything that contains information regarding Columbia State made or received in connection with operations, regardless of whether hard copy or electronic, and includes but is not limited to, written and printed matter, books, drawings, maps, plans, photographs, microforms, motion picture films, sound and video recordings, e-mails, computerized or other electronic data on hard drives or network drives, or copies of these items. See Record Retention Policy.

C. College technology resources means college-owned hardware, software, and network/communications equipment, technology facilities, and other relevant hardware and software items, as well as personnel tasked with the planning, implementation, and support of technology. College technology resources can be broken into the following categories:

   i. Campus network means the wired and wireless components and College technology resources connected to the network managed by the College's Office of Information Technology.
   ii. Device means a server, computer, laptop, tablet, or mobile device used to enter or

access College data from a College information system (i.e. Banner, Slate, SciQuest)

iii. College information system means an application or software used to support the academic, administrative, research, and outreach activities of the College, whether operated and managed by the College or a third-party vendor.

D. Effective Control means retaining physical possession of the device or securing the device in an environment such as a hotel safe, a bonded warehouse, or a locked and guarded exhibition facility.

E. Real-time scanning means the anti-virus software is always on and checks files in real time when created, opened, or copied.

F. Supported operating system means the entity providing the operating system (OS), be it a vendor, open source, or an individual, is actively and routinely providing and deploying patches and security updates for the OS.

i. Jailbroken means the process of modifying an iOS device such as an iPhone, iPad, or iPod Touch to bypass restrictions imposed by Apple to allow owner to modify the operating system, install non-approved applications, and grants the user elevated administration-level privileges.

ii. Rooted means the process of allowing Android users to attain privileged control over subsystems to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations otherwise inaccessible to a normal Android user.

## POLICY

I. Responsibilities

A. Individuals utilizing a personal device, including but not limited to smartphones, tablets, laptops, notebooks, and netbooks, to access College technology resources are responsible for the following:

i. Abiding by the requirements identified within this document;

ii. Configuring personal device(s) to connect to College technology resources;

iii. Any damages and criminal and/or civil charges resulting from the activities conducted on the personal device while connected to a College technology resource; and,

iv. All transactions made while authenticated by a College technology resource.

B. The College is not responsible or liable for the maintenance, backup, or loss of data on a personal device and does not accept responsibility for the security of personal devices including loss, theft, or damage.

C. The Office of Information Technology is responsible for College authentication systems, verifying authentication credentials provided, troubleshooting authentication issues, and performing vulnerability scans of the College network. The Office of Information Technology is NOT responsible for configuring use of personal devices to connect to College technology resources.

D. The Office of Information Technology is responsible for deploying all Campus Network infrastructure including wireless access points and routers.

II. Personal Device Use

A. Individuals who utilize a personal device to access College Technology Resources, whether for personal use, College business, on College Time, or during business travel must:

i. Abide by the acceptable use of technology resources and data policy;

ii. Ensure the physical security of the device to prevent loss, theft, and/or damage;

iii. Report lost or stolen devices that contained College Data; and ,

iv. Ensure the device meets the security requirements identified within Section 3 of this document.

B. A personally owned device must never disrupt use or function of the campus network and/or College Information System to which it is connected. The College will ban or prevent any device from accessing the campus network that continually causes disruptions of Information Technology resources.

C. The device owner must change their Columbia State password immediately when a personal device that has access to college systems or data is lost or stolen.

D. Authentication is required before a device will be permitted to access the student or employee network.

E. A personally owned device must never be used in order to circumvent security controls put in place by the Office of Information Technology.

III. Device Security

A. To prevent others from obtaining unauthorized access, device must remain under the owner's effective control at all times.

B. All devices that connect to Columbia State technology resources and/or access College data must meet the following requirements:

i. Employ an active form of access protection such as a passcode, passphrase, facial recognition, or fingerprint;

ii. Passwords/passphrases must meet the minimum requirements identified within the Password Standard;

iii. Have an anti-virus software installed and running real-time scanning and/or scan the device regularly to prevent, detect, and remove malware.

   iv. Be configured to lock or logout and require a user to re-authenticate if left unattended for more than 15 minutes. Devices that do not support this capability must be secured alternatively such as restricting access in a locked room;

C. Devices that are jailbroken, rooted, or have been subject to any other method of changing built-in protections must not be used to access College Technology resources.

D. Device must support WPA2 and AES to connect to student and/or employee networks.

IV. Conducting College Business

A. Pursuant to the Acceptable Use Policy, the College provides the use of technology resources, including devices, which must be used by authorized individuals as the primary means to create, store, send, or receive College data.
   i. *De minimis* use of personally owned devices is permitted to access College data and/or conduct College business provided the device meets the security requirements identified within section III.
   ii. Use of a personal device as the primary means to create, store, send, or receive college data is prohibited.
   iii. Employees who access sensitive data for their job must primarily use a College device. If a College device is not available, a personally owned device may be used for isolated incidents and is utilizing an approved College remote access solution to access sensitive data.

B. Software licensed to the College must never be downloaded to a personally owned device unless specifically permitted by the license (i.e. Office 365).

C. College data subject to document requests or document production stored on a personally owned device must be produced upon the request of the College.

D. Any College data downloaded to personally owned devices must be destroyed, removed, or returned to the College once the individual:

   i. Is no longer employed by Columbia State.
   ii. No longer requires access to the College data due to changing job responsibilities; or,
   iii. Is no longer the owner or primary user of the device.

V. Exceptions

A. Anti-virus software is not required to be installed on mobile devices such as cellphones and tablet computers.

*New policy March 2025, reviewed/accepted by the Cabinet, approved and signed by the President, March 2025.*