

POLICY: 6Hx28:7A-03



Responsible Executive: ~~Executive Vice President, Administrative Services~~
Chief Information Officer

Policy Contacts: Managing Dir, CISO

Specific Authority: 1001.64, F.S.

Law Implemented: 1001.64, F.S.

Effective Date: ~~03-12-2002~~09-11-2025

Date of Last Policy Review:

~~03-12-2002~~09-11-2025

Computer Hardware and Software Standards

Policy Statement:

I. In order to provide the highest possible level of computer support and functionality across all Valencia College ("College") facilities, the College shall develop and maintain computer hardware and software standards. These standards are documented in the implementing procedures document entitled, "Computer Hardware and Software Standards." These standards are intended to support the learning mission of the eCollege and to promote efficiency in response to user needs, cost effectiveness and fiscal responsibility in purchasing, and ease of administration of eCollege computer hardware and software resources. These standards shall be applied on a college-wide basis to develop and encourage an environment where resources may be shared rather than duplicated, while maintaining the flexibility to address unique computing needs among individual departments at the eCollege. -All ~~Valencia~~ College ~~faculty and staff~~employees shall comply with the standards as set forth in the "Computer Hardware and Software Standards".

~~I.II.~~ The College President or designee(s) may adopt procedures to implement this policy.

Related Documents/Policies:

Computer Hardware and Software Standards

Policy History:

Procedures:

I. Guidelines for Computer Hardware and Software Purchasing and Configuration

- A. All technology purchases (hardware or software) must be quoted and/or approved by the Office of Information Technology (OIT). There may be instances where OIT may not be able to source a quote for purchase. In those cases, a review of the technology must be conducted by OIT with approval granted prior to purchase by the respective department.
- B. OIT has a standard technology package made up of fully tested OIT-approved hardware and peripherals (e.g., desktop/laptop, monitors, docking station, keyboard, mouse). Departments may use the quote request form, available at <https://valenciacollege.edu/ITHelp>, to submit a request for any piece of hardware/peripheral(s) that are already approved by OIT. If the request includes items outside of the technology package (including different laptop model, peripherals, etc.) the requestor may still submit a quote request form to OIT for review and approval, as applicable.
 - 1. Requests for external hard drives or any form of external storage will require a review of the use case for external storage.
 - 2. Requests for devices requiring special wireless connectivity or a physical connection to the College network may require additional service(s) or infrastructure purchase(s) to facilitate limitations of capacity and/or sufficient segmentation to ensure the security of the College-wide network.
- C. To ensure proper hardware configuration, software compatibility, and the ability to provide technical support, all requests for acquisition of computer and network equipment, including servers and printers, must adhere to the following procedures:
 - 1. Any desktop or laptop computer system listed on the OIT validated systems list may be requested without contacting OIT or the Chief Information Officer (CIO) for review and/or approval.
 - 2. Any desktop or laptop computer system not listed on the OIT validated systems list must first be reviewed and approved by OIT.
 - 3. Any desktop or laptop computer system configuration request must be coordinated with OIT to determine if OIT support will be required for installation and setup, to include related scheduling and delivery commitments.

D. A list of approved and validated software at the College is located in the Software Center / Software Center for Apple Devices (<https://valenciacollege.edu/ITHelp>). All College employees with OIT-managed systems may install any application listed in the Software Center directly on their issued computer without needing to submit a service request to the OIT Service Desk.

1. To purchase software that is not available in the Software Center, a request must be submitted for review and approval by OIT. This includes but is not limited to all mobile, web-only, and “free” applications/sites. Any terms of service, terms and conditions associated with a piece of software or service, and/or potential privacy policy or regulation implications (e.g., FERPA, GLBA, PCI, HIPAA, CJIS), the specific term(s) and/or condition(s) will need to be provided with the request for review by the College’s contract, legal, and information security departments. Requests may be made through the OIT Support Portal (<https://valenciacollege.teamdynamix.com/TDClient/2067/Portal/Home/>).

E. Printers

1. The Employee Multi-Functional Device (MFD) Fleet on site at the College is centralized and managed by the Procurement Office. These MFDs provide printing, scanning, and copying functions. Details of these services and related services is available at the Procurement Office site at: <https://valenciacollege.edu/employees/procurement/printing-services.php>.
2. Requests for a desktop printer must be submitted for review and approval through the Procurement Office at valenciaprocurement@valenciacollege.edu.

F. Personal/Home Computers

1. OIT does not support computers purchased for personal use, with connectivity to College services. OIT will attempt to answer any questions over the phone that relate to connectivity to College services, such as Office365 and MyVC.
2. Any personally owned device(s) used to access College data or information technology resources must comply with the following minimum-security specifications.
 - a. The device(s) must be maintained at a current Vendor supported operating system(s).
 - b. The device(s) operating system(s) must be Original Equipment Manufacturer (OEM) issued and supplied by the vendor.
 - c. The device(s) must have passcode and screen lock enabled.

- d. Passwords and passcodes for the device(s) must meet the complexity requirements of the College.
- e. Multi-factor Authentication must be enabled (where applicable) on the device(s) when accessing College data.
- f. The device(s) must support encryption and enabled to protect any data that may be stored on the device(s).
- g. Any lost or stolen device(s) must be reported to OIT.
- h. All data must be removed from the device(s) before it is repurposed or no longer used to access the College's systems.
- i. Any device(s) that access the College's data and/or network may be removed and/or College account data wiped at the College's discretion.
- j. Access to some College applications or network locations may not be available.

G. Prohibited Technologies

- 1. The College has the discretion to restrict access to certain social media applications (apps) and sites when using a College-issued device or when personal devices are connected to the College network. These include but are not limited to: TikTok, WeChat, VKontakte, and Kaspersky. For more information, see *Prohibited Technologies at the College* on the OIT Knowledgebase of the College website.

II. Method and Level of Hardware Support

- A. Computers supplied to College employees will be supported through the OIT Service Desk and Campus Technology Services teams. Computers in academic labs, classrooms, and Learning Support will primarily be supported by their respective department or lab personnel, with the baseline configuration, software deployment, and security patching will be administered by members of the OIT Enterprise Storage and Systems team.
- B. OIT will provide primary support for all file and application servers that it manages. File and application servers managed by other areas are primarily the responsibility of their respective department or lab personnel, although baseline configurations and security may be administered by OIT unless there are extraordinary circumstances where the server is adequately segmented from the College-wide network.
- C. The College's security standards for servers applies to all College-owned devices, regardless of which department administers the system.

III. Support for Computer Hardware (Workstation) Platforms

- A. The Office of Information Technology (OIT) will provide official support for College purchased Windows-based and Apple (MacOS) computer systems, including non-standard computer systems that may need to be purchased for specialized functions and/or applications. Official support for non-standard systems will only be provided when such hardware environments have been approved in advance by the Chief Information Office (CIO) or their designee.
- B. Computers supplied to College employees, or other authorized individuals, for office work and administrative applications must possess certain functionality and should be compatible across all networks, departments, and campuses to facilitate ease of communication and use of college-wide applications.
 - 1. Academic system requirements should be based on the required functionality of the academic area or academic program that those systems will support.
 - 2. In some circumstances, conflicts may occur between required academic and administrative software on computer systems. In those cases, the College will attempt to provide a solution to the conflict and/or suggest alternative configurations.

IV. Support for File and Application Server Platforms

- A. OIT is responsible for approving all file and application servers that connect to the College's network infrastructure. To ensure the integrity and security of the College's overall network infrastructure, approved file and application servers will be subject to network and security configurations as required by OIT.
 - B. Only file and application servers that have been previously coordinated and approved by OIT will be supported by OIT.
- V. For additional questions, guidance, or support for computer hardware and/or software, individuals may contact OIT at 407-582-5555 or OITServiceDesk@valenciacollege.edu.

Procedure History:

Adopted 6-15-83; Amended 11-18-92; Amended 3-12-02; Amended 09-11-2025; Formerly 6Hx28:04-38.03

Date of Last Policy Review: ~~03-12-2002~~09-11-2025