POLICY: 6Hx28:7A-02

Responsible Executive: Executive Vice President, Administrative Services

Policy Contacts: Managing Director, Information Security

Specific Authority: 1001.64, F.S.
Law Implemented: Chapter 815, F.S.; 1001.64, F.S.; Title 18 of the U.S. Code; Electronic Communications Privacy Act of 1986 (ECPA)

Effective Date: 09-05-2024

Date of Last Policy Review: 09-05-2024

Acceptable Use of Information Technology Resources

Policy Statement:

I. Computing devices, networks, software, and institutional data are essential resources for accomplishing Valencia College's ("College") mission of teaching and learning. The College grants members of the College community shared access to these information technology resources in support of accomplishing the College's mission.

II. By using the College's information technology resources, authorized technology users ("users") agree to use these resources in a responsible and ethical manner, to abide by all relevant College policies and procedures, and adhere to applicable laws, rules, and regulations. These include, but are not limited to:

   A. College policies and procedures related to discrimination, harassment, and related misconduct; plagiarism; commercial use; information security, and ethical conduct; and

   B. Applicable laws, rules, and regulations relating to theft, copyright and licensing infringement, unlawful intrusions, and data privacy.

III. Members of the College community are granted access to information technology resources in order to facilitate their College-related academic, research, and employment activities. This access is a privilege, and users should not expect privacy in the use of

College resources. The College reserves the right to monitor the use of its information technology resources to ensure compliance with this policy and those procedures therein. Technology access for any user may be limited, suspended, and/or rescinded for any reason determined to be in the best interest of the College, including, but not limited to, emergency situations and/or violations of College policy(ies) and applicable laws, rules, and regulations, as appropriate. The College President or designee is authorized to impose disciplinary actions for students and employees, up to and including expulsion for students or dismissal from employment for employees, and referral to law enforcement for violations of standards of conduct required by this policy, as appropriate.

IV. The College President or designee(s) may adopt and amend procedures to implement this policy.

Policy History:

Adopted 6-15-83; Amended 11-18-92; Amended 3-12-02; Amended 9-05-2024; Formerly 6Hx28:04-38.02

Related Documents/Policies:

College Policy 6Hx28: 02-02 Discrimination, Harassment, and Related Misconduct

College Policy 6Hx28: 3E-05.2 Ethical Conduct and Performance

College Policy 6Hx28: 3E-08 Disciplinary Action

College Policy 6Hx28: 8-03 Student Code of Conduct

Guidelines for Selecting a Secure Password

Procedures:

I. User Responsibilities

A. Users are responsible for:

1. reviewing, understanding, and complying with all College policies and procedures and applicable laws, rules, and regulations related to access, acceptable use, and security of college information technology resources;

2. accessing only accounts, files, and data that are their own, that are publicly available, or to which they have been given authorized access; and appropriate use of such access. Accessing technology accounts includes safe computing practices, including but not limited to, users:

a. securing their passwords, not sharing their passwords with others, routinely

changing passwords, and not allowing the use of their account by others;

b. following guidelines to prevent unauthorized use by others;

c. signing off or securing systems from unauthorized use when vacating computer workstations; and

d. ensuring their workspace is secure if working onsite or remotely to avoid any intentional or accidental viewing of sensitive material. Remote users must ensure computing devices are connected to secure and encrypted networks and the College's VPN service is used for accessing any sensitive or protected systems or data.

3. securing information that is within the scope of the user's authorized access. The confidentiality of certain information such as student educational records or any other information considered to be sensitive or confidential shall be maintained and such information shall not be disclosed or distributed except in accordance with applicable College policies and applicable law, rules, and regulations.

4. asking systems administrators or data custodians for clarification on access and acceptable use issues or questions not specifically addressed in College policies, rules, guidelines, and/or procedures; and

5. reporting account intrusions, security compromises, suspicious cyber activity, or potential policy violations to the Office of Information Technology (OIT) at 407-582-5555 or OITServiceDesk@valenciacollege.edu for evaluation and action, as appropriate.

B. Users are required to use multi-factor authentication (MFA) for all College systems that may contain or access sensitive or confidential data, which includes but is not limited to the College portal, email, network, and cloud storage services. MFA is also required for and is not limited to:

1. all remote access via virtual private network (VPN); and

2. all system administration accounts used to access enterprise systems, storage devices hosted on campus, and sanctioned cloud environments.

C. To help maintain the proper functioning of computer and networking hardware and software, the College will take reasonable steps to ensure its computing resources are properly working and free of deliberately destructive software, such as viruses. Individuals must share responsibility for protecting College computers and must ensure the integrity of any electronic media they introduce.

1. Users must use only legal versions of copyrighted software on College owned computer or network resources, in compliance with vendor license

requirements.

2. Users must be able to document ownership, license rights or exceptions to license rights of software in their possession, with the assistance of the College in cases of college-installed software.

3. Copying or using software, except as explicitly permitted under licensing agreements, is a violation of the law and a user may be held accountable for such action(s).

D. Users should be aware of any conditions attached to or affecting the provision of College technology services, refrain from monopolizing systems, overloading systems, or networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

E. Personal Devices: The use of personal devices must be authorized for use with College information technology resources and must comply with the minimum security standards posted on the College website, *IT Help Knowledge Base*, which may be updated from time to time.

F. Users of College information technology resources are responsible for the content of their personal communications. The College accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

G. Employee and Contractor Training: All employees and contractors with access to College information technology resources must complete the *Information Security at Valencia College* awareness training through the Valencia EDGE portal within the first 30 days of their initial hire and annually thereafter. Other training may be required for employees with access to specific data or systems, as applicable.

II. Prohibited Uses:

A. The computing and network resources of the College may not be used:

1. to impersonate another person or misrepresent authorization to act on behalf of others or the College, which includes but is not limited to the unauthorized use or fraudulent use of another individual's user ID and/or password;

2. to create or distribute digitally altered images, video, written text, and/or audio (e.g., deepfakes) for disinformation, deceptive misuses, and/or other misconduct in violation of applicable College policies and procedures, and where appropriate, local, state, and federal laws, rules, and regulations.

3. for personal financial gain or commercial purposes except as expressly allowed by College policy(ies);

4. for inappropriate conduct that is considered a violation of College Policies 6Hx28: 2-01 Discrimination, Harassment, or Related Misconduct, 3D-05.2 Ethical Conduct and Performance, and/or 8-03 Student Code of Conduct. This includes but is not limited to creating, downloading, viewing, posting, storing, printing, and/or transmitting to others images, sounds, or messages that might be perceived by a reasonable person as, or have been identified to be in violation of any of the policies listed within this section.

5. to violate any other College policies and/or procedures; or

6. for any illegal activity.

B. Users and other individuals must not intentionally damage or disable computing systems, networks, or software or attempt to undermine the security or the integrity of computing systems or networks and must not attempt to gain unauthorized access. Users may not use any computer program or device to intercept or decode passwords or similar access control information. If security gaps are observed, they should be reported to the Office of Information Technology (OIT) at 407-582-5555 or OITServiceDesk@valenciacollege.edu for evaluation and action, as appropriate.

C. The College recognizes incidental personal use of College information technology resources, as long as this use does not interfere with the performance of the user's job duties or responsibilities, does not consume a significant amount of those resources, and does not violate any other College policies or procedures.

III. Expectation of Privacy

A. Although the College takes reasonable security measures to protect the security of its computing resources and accounts assigned to individuals, the College does not guarantee absolute security and privacy for its users. The College assigns responsibility for protecting its resources and data to system administrators and data custodians, who treat the contents of individually assigned accounts and personal communications as private and does not examine or disclose the contents except:

1. as required for system maintenance including security measures;

2. when there exists reason to believe an individual is violating College policy and/or laws, rules, and/or regulations, as appropriate; and/or

3. as permitted by applicable College policy(ies) and applicable laws, rules, and regulations.

B. Most written communications using College computing resources are subject to Florida Public Records Law, Chapter 119, F.S., with some exceptions. For

purposes of compliance with requirements of Florida statutes, the Office of the Director, Contracts and Records is designated as the general Custodian of Public Records. For questions or more information pertaining to public records and written communications using College computing resources, contact the Director of Contracts and Records at 407-582-3465 or publicrecordsnotice@valenciacollege.edu.

IV. Reporting Violations

A. All information technology resources are supplied to users for the performance of essential job functions and academic purposes. These resources must be used in a manner consistent with this policy and applicable laws, rules, and regulations.

B. The College reserves the right to copy and examine any files or information resident on College systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Access privileges to the College's information technology resources will not be denied without cause.

C. Reports of alleged policy and/or procedure violations should be reported to the Office of Information Technology (OIT) at 407-582-5555 or OITServiceDesk@valenciacollege.edu for initial evaluation. Based on the nature and severity of the allegations, OIT will partner with either Organizational Development and Human Resources or the Office of Student Rights and Responsibilities, as appropriate, if a College inquiry, investigation, or further assistance is needed.

1. During the initial evaluation, if it appears necessary to protect the integrity, security, and/or continued operation of its computers and networks, or to protect itself from liability, the College may temporarily restrict access to those resources.

2. If it is determined that a violation has occurred and depending on the nature and severity of the offense, violators of this policy and/or its implementing procedure may be subject to additional and appropriate College action, including but not limited to, College disciplinary action, denial of access to College property, and/or criminal prosecution under applicable laws, rules, and regulations. For more information, see College Policies 6Hx28: 3E-08 Disciplinary Action and 8-03 Student Code of Conduct.

Procedure History:

Adopted 6-15-83; Amended 11-18-92; Amended 03-12-02; Amended 9-5-2024; Formerly 6Hx28:04-38.02

Related Documents/Procedures:

IT Knowledge Base

Date of Last Procedure Review: 09-05-2024