POLICY: 6Hx28:7A-01

Responsible Executive: Executive Vice President, Administrative Services

Policy Contact: Managing Director, CISO

Specific Authority: 1001.64, F.S.

Law Implemented: 501.171, F.S.; Family Educational Rights and Privacy Act (FERPA); General Data Protection Regulation (GDPR); Gramm-Leach-Bliely Act (GLBA); Health Insurance Portability and Accountability Act (HIPAA); Red Flags Rule

Effective Date: 03-13-2025

Date of Last Policy Review: 03-13-2025

Information Security Program

Policy Statement:

I. Valencia College ("College") is committed to security, confidentiality, integrity, availability, and accountability with regard to the personal and sensitive information it collects, creates, uses, and maintains. The College shall take reasonable measures to protect and secure data containing such information in accordance with applicable laws, rules, regulations, and College policies. This policy defines, documents, and supports the implementation and maintenance of the College's information security program comprised of administrative, technical, and physical safeguards to:

   A. Protect against any anticipated threats or risks to the security, confidentiality, integrity, or availability of personal or sensitive information; and

   B. Protect against unauthorized access to or use of College-maintained personal or sensitive information that could result in substantial harm or inconvenience to any its students or employees.

   C. Provide timely, reliable, authorized, and relevant access to data, including personal or sensitive information, to College faculty and staff appropriate to their respective position at the College.

II. This policy applies to all members of the College, or those working on its behalf, who may be

granted access to or responsible for maintaining College information resources to include any records that contain personal or sensitive information in any format.

III. The College has designated the Chief Information Security Officer to implement, oversee and enforce the College's information security program ("program"). This role is responsible for the:

A. Initial implementation of the program based on cybersecurity standards appropriate and applicable to the College;

B. Engagement of qualified information security personnel to include providing them with security updates and training sufficient to address relevant risks;

C. Training to applicable employees, contractors, and other stakeholders to effectively safeguard the information resources they have been granted access to or otherwise responsible for maintaining;

D. Review of this policy, procedure, and the security measures defined on a regular basis, including without limitation, when indicated by the College's risk assessment or program monitoring and testing activities, or when there is a material change to the College's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of information resources containing personal or other sensitive information, and implement updates as needed;

E. Development and management of an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate requests for deviations from this policy or other College information security policies and procedures.

F. Periodic reporting to the College's District Board of Trustees and senior leadership regarding the status of the information security program and the College's safeguards to protect personal and other sensitive information.

IV. Members of the College community are granted access to information and information technology resources to facilitate their College-related academic, research, and employment activities, as applicable. 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 as appropriate, referral to law enforcement for violations of standards of conduct required by this policy and its implementing procedures.

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

Policy History:

Adopted 03-13-2025

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: 7A-02 Acceptable Use of Information Technology Resources

College Policy 6Hx28: 7B-01 Preservation and Disposal of Records

College Policy 6Hx28: 7B-02 Student Records

College Policy 6Hx28: 7B-04 Financial Information Security

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

Procedures:

I. Definitions:

A. Personal Information: Any of the following, including but not limited to:

1. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

a. A social security number or Florida Education Identifier (FLEID) number;

b. A driver license or identification card number, password number, military identification number, or other similar number issued on a government document used to verify identity;

c. A financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

d. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

e. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual;

f. An individual's biometric data, which means data generated by automatic measurements of an individual's biological characteristics;

g. Any information regarding an individual's geolocation such as physical location, internet protocol (IP) address, or other location information.

2. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

3. Any personally identifiable financial information or list, description, or other grouping

that is derived using any personally identifiable financial information that is not publicly available.

B. Sensitive Information: Data that:

1. is confidential and exempt pursuant to Florida public records laws, including without limitation, student education records, health records, and limited access employee records.

2. if accessed by or disclosed to unauthorized parties, could cause significant or material harm to the constituents of the College.

II. Risk Assessment: The College will conduct and base the information security program on a periodic, documented risk assessment, at least annually, or whenever there is a material change in the College's business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information.

A. The risk assessment shall:

1. Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal or other sensitive information and include criteria for evaluating and categorizing those identified risks;

2. Define assessment criteria and assess the likelihood and potential damage that could result from such risks, including the unauthorized disclosure, misuse, alteration, destruction, or other compromise of the personal or other sensitive information, taking into consideration the sensitivity of the personal and any other sensitive information; and

3. Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

a. Employee, contractor, and (as applicable) stakeholder training and management;

b. Employee, contractor, and (as applicable) stakeholder compliance with this policy and related policies and procedures;

c. Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and

d. the College's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

B. Following each risk assessment, the College will:

1. Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks, as applicable;

2. Address any identified gaps, including documenting the College's plan to remediate,

mitigate, accept, or transfer identified risks, as appropriate; and

3. Regularly monitor the effectiveness of the College's safeguards, as specified in this policy and procedure.

III. Policies and Procedures: The College will develop, maintain, and distribute information security policies and procedures on a periodic basis and in accordance with applicable laws, rules, regulations, and standards to relevant employees, contractors, and (as applicable) other stakeholders.

IV. Information Security Awareness and Training Program: The College will establish and maintain an information security awareness and training program to inform the users of College's information and information technology resources in a secure and ethical manner.

A. 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.

B. The content of the Information Security training required of employees and contractors will be reviewed and updated on an annual basis to ensure currency and applicability to the regulations, laws and standards that apply to the College, which may be updated from time to time.

V. Safeguards

A. The College will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal and other sensitive information that the College owns or maintains. These safeguards shall be appropriate to our size and scope, our available resources, and the amount of personal and other sensitive information we own or maintain.

B. The College's safeguards shall, at a minimum, include but are not limited to:

1. Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the College to successfully carry out its assigned duties.

2. Perform access control reviews of College information technology assets ("assets") to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently as needed.

3. Require authentication for access to all College assets, including the College network, computers, servers, appliances, and services hosted by the College or an authorized third-party. Authentication is also required for external access to all non-public College network and Internet services.

a. Directory services will be used as the source of network authentication.

b. All departments that accept remote modem calls must also require directory services user names and passwords for authentication, which does include services hosted or offered to the College that may be used to access, store, process, or transmit College data.

c. Any third-party service or system that cannot use the College Directory services, via single-sign-on (SSO) will require compensating controls to ensure that authentication and accounts are managed in a similar manner and to the same security level as systems connected to the College Directory services.

4. Establish and maintain an accurate, detailed, and up-to-date inventory of all College assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT (Internet of Things) devices, and servers. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the College's network infrastructure, even if they are not under control of the College.

   a. Inventory records should include the network address (if static), hardware address, machine name, College asset owner, department for each asset, and whether the asset has been approved to connect to the network.

   b. For mobile end-user devices, mobile device management (MDM) type tools may be used to support the safeguard process, where appropriate.

   c. Inventory of all College assets shall be reviewed and updated bi-annually, or more frequently as needed. This inventory includes:

      i. assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments; and

      ii. assets that are regularly connected to the College's network infrastructure, even if they are not under control of the College.

5. Encryption

   a. Encrypt sensitive data in transit. Example implementations may include but are not limited to: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

   b. Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data.

      i. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this safeguard.

      ii. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

6. Secure Development Lifecycle

a. Establish and maintain a secure application development process to address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Documentation shall be reviewed annually and updated as needed, or when significant College changes occur that could impact this safeguard.

b. Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process will include such items as: a vulnerability handling procedure that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. The software vulnerabilities documentation will be reviewed annually and update as needed, or when significant College changes occur that could impact this safeguard.

c. Inform third-party application developers of the College's policy expectations of the secure development lifecycle for outside stakeholders.

d. Perform root cause analysis on security vulnerabilities to evaluate underlying issues that may create vulnerabilities in code to allow development teams to in addition to correcting individual vulnerabilities as they arise.

7. Multifactor Authentication (MFA)

a. Require all externally-exposed College or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this safeguard.

b. Require MFA for remote network access.

c. Require MFA for all administrative access accounts, where supported, on all College technology assets, whether managed on-site or through a third-party provider.

8. Securely dispose of data as outlined in the College's data management/retention policies and procedures. Ensure the disposal process and method are commensurate with the data sensitivity.

9. Adopt procedures for change management which may include but are not limited to: security patching; configuration changes; firewall rules changes; application development, deployment, and maintenance; system and application upgrades; and other critical infrastructure changes.

10. Audit Log Management

a. Establish and maintain an audit log management process that defines the College's logging requirements that include at a minimum, the collection, review, and retention of audit logs for College technology assets.

b. Review and update asset documentation annually, or when significant College changes occur that could impact this safeguard.

c. Collect audit logs and ensure that logging, per the College's audit log management process, has been enabled across College assets.

d. Configure detailed audit logging for College assets containing sensitive data that includes event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

VI. The College will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain personal or other sensitive information on its behalf by:

A. Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this policy and all applicable laws and the College's obligations.

B. Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this policy and all applicable laws and the College's obligations.

C. Monitoring and periodically auditing the service provider's performance to verify compliance with this policy and all applicable laws and the College's obligations.

VII. Monitoring of the Information Security Program

A. The College will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal or other sensitive information. The College shall reasonably and appropriately address any identified gaps.

B. The College will establish and maintain a vulnerability management program for College assets, to include:

1. Performing operating system and application updates on College assets through automated patch management on a month, or more frequent, basis;

2. Performing automated vulnerability scans of internal College assets on a quarterly, or more frequent, basis;

3. Performing automated vulnerability scans of externally-exposed College assets on a monthly, or more frequent, basis; and

4. Remediate detected vulnerability in software on a monthly, or more frequent, basis.

C. The College will establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the College, to include:

1. Performing periodic external penetration tests, no less than annually, on the network, web applications, application programming interfaces (APIs), hosted services, and physical premise controls; and

2. Remediate penetration test findings base on the potential impact and severity of the

vulnerabilities found.

VIII. Incident Response.

A. The College will establish and maintain written policies and procedures regarding information security incident response. Such procedures shall include:

1. Documenting the response to any security incident or event that involves a compromise of security.

2. Performing a post-incident review of events and actions taken.

3. Reasonably and appropriately addressing any identified gaps.

IX. Reporting Violations

A. Reports of alleged violation(s) of the information security program policy, procedures, or other appropriate guidelines 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 Organizational Development and Human Resources and/or the Office of Student Rights and Responsibilities, as appropriate, if a College inquiry, investigation, or further assistance is needed.

B. 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 College technology access and/or College property; and/or criminal prosecution under applicable laws, rules, and regulations. For more information, see College Policies 6Hx28: 3E-08 Disciplinary Action and 6Hx28: 8-03 Student Code of Conduct.

Procedure History:

Adopted 6-15-83; Amended 11-18-92; Amended 3-12-02; Amended 3-13-2025; Formerly 6Hx28:04-38.02

Related Documents/Procedures:

IT Knowledge Base

Date of Last Procedure Review: 03-13-2025