**POLICY: 6Hx28:7B-04**

**Responsible Executive:** Chief Information Officer

**Policy Contacts:** Managing Director, CISO

**Specific Authority:** 1001.64, F.S.
**Law Implemented:** 1001.64, F.S.; Gramm-Leach-Bliely Act (GLBA); 16 CFR Part 314

**Effective Date:** 09-11-2025

**Date of Last Policy Review:** 09-11-2025

# Financial Information Security Program

**Policy Statement:**

I. In accordance with the Gramm-Leach-Bliley Act of 1999, also known as the Financial Services Modernization Act of 1999 (GLBA), together with the implementing "Safeguards Rule" issued by the Federal Trade Commission (16 CFR Part 314, Standards for Safeguarding Customer Information; Final Rule), which regulate the security and confidentiality of non-public customer personal information collected or maintained by or on behalf of financial institutions or their affiliates, and to the extent that Valencia College ("College") is classified as a financial institution under GLBA, by virtue of processing or servicing student or employee loans, or offering other financial products or services, the College shall establish a Financial Information Security Program ("Program") to assure compliance with GLBA and the Safeguards Rule. The Program shall be designed to provide safeguards for the security and confidentiality of non-public customer personal information,1[1] protect against anticipated threats or hazards to the security or integrity of such information and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to a customer. The Program shall also provide for mechanisms to:

A. Identify and assess the risks that may threaten covered data and information maintained by the College;

B. Develop written policies and procedures to manage and control these risks;

C. Implement and review the Program; and

D. Adjust the Program to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

II. Members of the College community are granted access to financial information and relevant technology resources to perform their job-related duties, as applicable. This policy applies to all employees of the College, or those external individuals or entities working on the College's behalf, who may be granted access to or responsible for maintaining College financial information resources to include any relevant records in any format.

III. The College President or designee(s) is authorized to impose appropriate College action for a violation(s) of standards of conduct required by this policy and its implementing procedures.

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

[1] Covered data and information for the purpose of this policy includes Non-public customer personal information (defined below) required to be protected under the Gramm Leach Bliley Act (GLB). In addition to this coverage which is required under federal law, Valencia College chooses as a matter of policy to also include in this definition any bank and credit card account numbers, income and credit information, tax returns, asset statements, and social security numbers received in the course of business by the College, whether or not such information is covered by GLB. Covered data and information includes both paper and electronic records.
Non-public customer personal information means any personally identifiable financial information, not otherwise publicly available, that Valencia has obtained from a student, student parent or spouse, employee, alumnus, or other third party, in the process of offering a financial product or service, OR such information provided to Valencia by another financial institution, OR such information otherwise obtained by Valencia in connection with providing a financial product or service. Offering a financial product or service includes such activities as student loans and other miscellaneous financial services as defined in 12 CFR Section 225.28. Examples of personally identifiable financial information include names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, in both paper and electronic form.

---

**Related Policies:**

College Policy 6Hx28: 7A-01 Information Security Program
College Policy 6Hx28: 3E-08 Disciplinary Action
College Policy 6Hx28: 8-03 Student Code of Conduct

---

**Policy History:**

Adopted 6-20-06; Amended 9-11-25; Formerly 6Hx28:06-30

---

**Procedures:**

I. The main elements of the Financial Information Security Program ("Program") are located within College Policy 6Hx28: 7A-01 Information Security Program. The College

has a designated program administrator to oversee, implement, and enforce the information security program, which includes the financial information program. The program administrator shall annually report to the College President on the effectiveness of the information security program, including financial information, and any recommended changes.

II. The College will periodically conduct a risk assessment that reasonably identifies internal and external risks, including third party service providers, affecting the confidentiality, integrity, and availability of customer information.

III. The College shall design and implement safeguards to control risks and threats identified by the risk assessment. Safeguards will be monitored for effectiveness and to detect actual or attempted attacks on, or intrusions into, financial information technology resources.

IV. In compliance with the GLBA and "Safeguards Rule", the Program shall include but not be limited to:

A. Identifying and managing financial data, information technology resources, and facilities, implementing safeguards to control the risks and threats to these assets reasonably commensurate to their level of importance and the material impact that may result from a compromise.

B. Implementing a multifactor authentication and related authorization and access controls to restrict access to financial information technology resources following the principles of least privileges and limiting users' access to only the customer information required for the user to perform their job duties and functions.

C. Adopting secure development practices for in-house developed applications used for transmitting, accessing, and storing customer information to include adopting procedures for evaluating, assessing or testing the security of externally developed applications used to transmit, access, or store customer information.

D. Encrypting all customer information maintained and in use by the College at rest and when in transit over external or public networks.

E. Securely disposing customer information within two years of last use, unless there is an applicable law, rule, regulation, or other valid business use for such information that would require extending the retention of customer information. Data retention policies, procedures, and practices will be periodically reviewed, as determined by the College, and maintained to minimize the unnecessary retention of data.

F. Establishing processes and procedures, as applicable, to monitor and log authorized user activity and detect unauthorized access, use, or tampering of

customer information, and the information technology resources used to collect, process, store, and transmit customer information.

G. Selecting and retaining service providers capable of maintaining appropriate safeguards for customer information (in accordance with internal processes). The College will oversee and contractually require service providers to implement the appropriate safeguards by establishing terms and conditions for service providers that collect, process, store, or transmit customer information. These terms and conditions shall include a provision allowing the College to obtain or review, upon request, the results of their latest penetration tests and vulnerability assessment.

H. Documenting and maintaining an incident response plan designed to promptly respond to and recover from security events that have an impact on customer information.

I. Adopting and implementing change management processes and procedures for all financial information technology resources maintained by the College.

J. Requiring all employees and contractors with access to College information technology resources to complete the Information Security at Valencia College awareness training in accordance with College Policy 6Hx28: 7A-01 Information Security Program. Additional financial information training is required for those with access to customer information, those that administer or manage the information technology resources or facilities that are used to collect, process, store, or transmit customer information, and those that are responsible for the securing of customer data.

K. Periodically evaluating at least annually or sooner (as appropriate) the Program as a result of a risk assessment, penetrating testing or vulnerability assessment(s), identifying new vulnerabilities or threats discovered in response to a security event, or any other circumstance(s) that may have a material impact to the Program.

V. Reporting Violations

A. 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.

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 procedures

may be subject to additional and appropriate College action, including but not limited to, College disciplinary action, denial of access to College networks and/or 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 6-20-06; Amended 9-11-25; Formerly 6Hx28:06-30

---

**Date of Last Procedure Review:** 09-11-2025