POLICY: 6Hx28:7B-04

Responsible Executive: Executive Vice President, Administrative Services

Policy Contacts:

Specific Authority: 1001.64, F.S.
Law Implemented: 1001.64, F.S.

Effective Date: 06-20-2006

Date of Last Policy Review:
06-20-2006

Financial Information Security

Policy Statement:

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 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 Plan to assure compliance with GLBA and the Safeguards Rule. The Plan 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 Plan shall also provide for mechanisms to:

I. Identify and assess the risks that may threaten covered data and information maintained by Valencia;

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

III. Implement and review the plan; and

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

1[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:

Policy 6Hx28:7A-02 Acceptable Use of Information Technology Resources
Policy 6Hx28:7A-05 User Authentication Requirements

Policy History:

Adopted 6-20-06; Formerly 6Hx28:06-30

Procedures:

I. Financial Information Security Plan Committee

The Director of Risk Management, who serves as Chair, the Assistant Vice President for Financial Services, the Assistant Vice President of Organizational Development and Human Resources, the Assistant Vice President for College Transition, the Director of Auxiliary Services, a Valencia Enterprises representative, and the Vice President, Information Technology and CIO, IT Office, have been appointed to serve on the Financial Information Security Plan Committee (the Committee) to coordinate the implementation of this Plan. They are responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to Valencia. The Internal Auditor will be responsible for conducting reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that Valencia departments comply with the requirements of this policy.

II. Identification and Assessment of Risks to Customer Information

A. Valencia recognizes that it has both internal and external financial information security risks. These risks include, but are not limited to:

1. Unauthorized access of covered data and information by someone other than the owner of the covered data and information

2. Compromised system security as a result of system access by an unauthorized person

3. Interception of data during transmission

4. Loss of data integrity

5. Physical loss of data in a disaster

6. Errors introduced into the system

7. Corruption of data or systems

8. Unauthorized access of covered data and information by employees

9. Unauthorized requests for covered data and information

10. Unauthorized access through hardcopy files or reports

11. Unauthorized transfer of covered data and information through third parties

B. Valencia College recognizes that this may not be a complete list of the risks associated with the protection of covered data and information, since technology growth is not static, and new risks are created regularly. Accordingly, the Office of Information Technology will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group and SANS to identify new risks.

C. Each College office or department handling covered data and information, as identified by the Committee, will take steps to identify and assess internal and external risks to the security, confidentiality, and integrity of covered data and information that could result in the unauthorized access, disclosure, misuse, alteration, destruction or other compromise of such information.

D. The risk assessment shall include consideration of risks, and assessment of the sufficiency of current safeguards to manage those risks, to covered data and information in each relevant aspect of College operations, including: employee,

student worker, and volunteer training and management regarding access to and use of such information; information systems (including network and software design, as well as information processing, storage, transmission and disposal for both paper and electronic records); and detecting, preventing and responding to attacks, intrusions, or other system failures (including data processing and telephone communication), as well as contingency planning and business continuity.

E. The Committee, with the assistance of the Office of Vice President for Policy and General Counsel and the Internal Auditor, will establish procedures for identifying and assessing risks and safeguards in each relevant area of the College's operations outlined above. The Committee will delegate the risk identification and assessment to the appropriate individual(s) within each affected office or department, who will be that office's contact person with the Committee.

1. Design, Implementation, and Monitoring of Safeguards

a. In consultation with the Committee, each affected office or department will design, implement, and maintain in writing, such administrative, technical, and physical safeguards as are necessary to control the risks identified through risk assessment, and will regularly monitor the effectiveness of such safeguards. Each office should design and implement safeguards in accordance with the nature and scope of that office's activities and the sensitivity of the covered data and information at issue. The contact person for each such office must provide a copy of the written safeguards to the Committee.

b. The Committee, with the assistance of the Office of Vice President for Policy General Counsel, will provide guidance on appropriate safeguards to all affected offices and departments, and will work with individual offices as requested or appropriate in the design and implementation of safeguards.

III. Design and Implementation of Safeguards Program

A. Employee Management and Training

References of new employees working in areas that regularly work with covered data and information including without limitation Business Office, Office of the Registrar, Auxiliary Services, Office of Information technology, Finance Office, and Financial Aid Office are checked. Every current employee and new employees during employee orientation, in these departments will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data and information. These same employees will sign a confidentiality agreement to indicate their understanding

and agreement with their privacy and safeguarding obligations. Each employee is also trained in the proper use of computer information and passwords. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling" 2[2] and how to properly dispose of documents that contain covered data and information. Each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. Further, each department responsible for maintaining covered data and information shall work with the Committee on an annual basis regarding additional privacy training appropriate to the department. These training efforts should help minimize risk and safeguard covered data and information security.

B. Physical Security

1. Valencia has addressed the physical security of covered data and information by limiting access to only those employees who have a business reason to know such information.

2. Loan files, account information and other paper documents are kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees know combinations and have access to keys. Paper documents that contain covered data and information are shredded at time of disposal.

C. Information Systems

1. Access to covered data and information via Valencia's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and distinct password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, are available only to Valencia employees in appropriate departments and positions.

2. Valencia will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data and information is secure and to safeguard the integrity of records in storage and transmission. All servers maintained and managed by the Office of Information Technology are administered in order to provide appropriate configuration, authentication, and security controls. This includes monitoring of such systems for unusual activity or unauthorized access, as well as maintenance of operating system and application security patches and upgrades. For servers manages outside of the Office of Information Technology, the responsible area administrator (Director, Dean, Campus Provosts, or Vice President) is held accountable for ensuring appropriate

configuration, authentication, and security controls, as well as monitoring of system activity and the timely application of security patches and upgrades. The Office of Information Technology shall maintain a separate form for each of these servers that indicates acceptance of these responsibilities by the responsible administrator. User and system passwords are also required to comply with the Valencia College Password Policy. In addition, an intrusion detection/prevention system has been implemented to detect and stop certain external threats, along with an Incident Response Procedure for occasions where intrusions do occur.

3. All covered data and information will be maintained on servers that are behind Valencia's firewall. All firewall software and hardware maintained by the Office of Information Technology will be kept current. The Office of Information Technology has a number of policies and procedures in place to provide security to Valencia's information systems. These policies are available upon request from the Office of Information Technology.

D. Management of System Failures

The Office of Information Technology has developed written plans and procedures to detect any actual or attempted attacks on Valencia systems and has an Incident Response Procedure which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This procedure is available upon request from the Office of Information Technology.

E. Selection of Appropriate Service Providers

1. GLBA requires the College to take reasonable steps to select and retain service providers who maintain appropriate safeguards for non-public customer personal information. In addition, Valencia will take reasonable steps to select and retain service providers who maintain appropriate safeguards for other covered data and information, whether or not required under GLBA. A "service provider" is any person or entity that receives, maintains, processes, or otherwise is permitted to access covered data and information through its provision of services directly to Valencia. The Vice President for Policy and General Counsel will develop standard, contractual provisions applicable to third-party service providers, which will require such providers to implement and maintain appropriate safeguards. All relevant future contracts between the College and these service providers should contain these provisions. Any deviation from these standard provisions will require prior approval.

2. The provisions may include:

a. An explicit acknowledgement that the contract allows the contract partner access to confidential information;

b. A specific definition or description of the confidential information being provided;

c. A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;

d. An assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;

e. A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;

f. An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles Valencia to terminate the contract without penalty;

g. A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement, and;

h. A right to audit clause.

F. Continuing Evaluation and Adjustment

This Financial Information Security Plan will be subject to periodic (at least annual) review and adjustment. The most frequent of these reviews will occur within the Office of Information Technology, where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the appointed Financial Information Security Plan Committee which will assign specific responsibility for implementation and administration as appropriate. The Committee, in consultation with the other appropriate offices, will review the Plan annually to assure ongoing compliance with GLBA and the Federal Trade Commission Safeguards Rule, as well as consistency with other existing and future laws and regulations. Also, it may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

G. Identity Theft Prevention Program

The District Board of Trustees ("Board") recognizes that some activities of Valencia College ("College") are subject to the provisions of the Fair and Accurate Credit Transactions Act (FACT Act) and its "Red Flag" rules. Therefore, the Board adopts on this 27th day of October, 2009, the following initial Identity Theft Prevention program for College.

1. Program Adoption. The Board hereby adopts this initial Identity Theft Prevention Program ("Program") in compliance with the "Red Flag" rules issued by the Federal Trade Commission pursuant to the FACT Act. The College is engaging in activities which are covered by the FACT Act Red Flag rules. After consideration of the size and complexity of the College's operations and account systems, and the nature and scope of the College's activities, the Board has determined that this Program is appropriate for the College.

2. Program Purpose. Under the Red Flag rules, the College is required to establish an "Identity Theft Program" with reasonable policies and procedures to detect, identify, and mitigate identity theft in its covered accounts. The Program shall include reasonable procedures to:

    a. Determine the applicability of Red Flags Rules to the College;

    b. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;

    c. Detect red flags that have been incorporated into the Program;

    d. Respond appropriately to any red flag that are detected to prevent and mitigate identity theft; and

    e. Ensure the Program is updated periodically to reflect changes in risks to students and employees, and creditors from identity theft.

3. Responsible College Official. The President shall designate the Vice President of Business Operations and Finance to serve as Program Administrator. The Program Administrator shall exercise appropriate and effective oversight over the Program and shall report regularly to the President on the Program.

4. Program Administration and Maintenance. The Program Administrator is responsible for developing, implementing and updating the Program throughout the College system. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red

Flags and the steps for identifying, preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

5. The Program will be periodically reviewed and updated to reflect changes in identity theft risks and technological changes. The Program Administrator will consider the College's experiences with identity theft, changes in identity theft methods; changes in identity theft detection, mitigation and prevention methods; changes in types of accounts the College maintains; changes in the College's business arrangements with other entities, and any changes in legal requirements in the area of identity theft. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted.

6. The Program Administrator shall confer with all appropriate College personnel, Councils and committees as necessary to ensure compliance with the Program. The Program Administrator shall annually report to the President on the effectiveness of the Program. The Program Administrator shall present any recommended changes to the President for approval. The President's approval shall be sufficient to make changes to the College Identity Theft Program.

7. Definitions. Pursuant to the Red Flag regulations at 16 C. F. R. § 681.2, the following definitions shall apply to this Program:

    a. "Covered accounts":
        i. Any account the College offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions.

        ii. Any other account the College offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the College from Identity Theft.

    b. "Credit": The right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefor.

    c. "Creditor": An entity that regularly extends, renews, or continues credit.

    d. "Customer": Any person with a covered account with a creditor.

e. “Identifying information”: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including:

i. name
ii. address
iii. telephone number
iv. social security number
v. date of birth
vi. government issued driver’s license or identification number
vii. alien registration number
viii. government passport number
ix. employer or taxpayer identification number
x. unique electronic identification number
xi. computer’s Internet Protocol address or routing code

f. “Identity Theft”: An attempted or committed fraud using the identifying information another person without permission.

g. “Red Flag”: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

8. Identification of Red Flags. In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The following are relevant Red Flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

a. Notifications and Warnings from Credit Reporting Agencies

i. Report of fraud accompanying a credit report;

ii. Notice or report from a credit agency of a credit freeze on a customer or applicant;

iii. Notice or report from a credit agency of an active duty alert for an applicant; and

iv. Indication from a credit report of activity that is inconsistent with a customer’s usual pattern or activity.

b. Suspicious Documents

i. Identification document or card that appears to be forged, altered or inauthentic;

ii. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

iii. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and

iv. Application for service that appears to have been altered or forged.

c. Suspicious Personal Identifying Information

i. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);

ii. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);

iii. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

iv. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

v. Social security number presented that is the same as one given by another customer;

vi. An address or phone number presented that is the same as that of another person;

vii. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and

viii. A person's identifying information is not consistent with the information that is on file for the customer.

d. Suspicious Account Activity or Unusual Use of Account

i. Change of address for an account followed by a request to change the account holder's name;

ii. Payments stop on an otherwise consistently up-to-date account;

iii. Account used in a way that is not consistent with prior use (example: very high activity);

iv. Mail sent to the account holder is repeatedly returned as undeliverable;

v. Notice to the College that a customer is not receiving mail sent by the College;

vi. Notice to the College that an account has unauthorized activity;

vii. Breach in the College's computer system security; and

viii. Unauthorized access to or use of customer account information.

e. Alerts from Others

Notice to the College from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

9. Detecting Red Flags. The Program's general Red Fag detection practices are described in this document. The Program Administrator will develop and implement specific methods and protocols appropriate to meet the requirements of this Program.

a. Veterans' deferments of tuition payments

i. New Accounts. In order to detect any of the Red Flags identified above associated with the opening of a new account, College personnel will take the following steps to obtain and verify the identity of the person opening the account:

a) Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;

b) Verify the student's identity (for instance, review a driver's license or other identification card);

c) Independently contact the student.

ii. Existing Accounts. In order to detect any of the Red Flags identified above for an existing account, College personnel will take the following steps to monitor transactions with an account:

a) Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);

b) Verify the validity of requests to change billing addresses; and

c) Verify changes in banking information given for billing and payment purposes.

b. Consumer Reports. In order to detect any of the red flags identified above for a prospective employee for which a consumer credit report is required, College personnel will take the following steps to assist in identifying address discrepancies:

i. Require written verification from any applicant that the address provided by the applicant is accurate at the request for the credit report is made to the consumer reporting agency.

ii. In the event that notice of an address discrepancy is received, verify the credit report pertains to the prospective employee for whom the requested report was made, and report to the consumer reporting agency an address for the prospective employee that the College has reasonably confirmed is accurate.

c. Tuition installment payment plan ("TIP")

10. Students must contact outside service provider and provide personally identifying information to them. (See Oversight of Service Provider Arrangements section).

a. Responding to Red Flags and Mitigating Identity Theft. In the event College personnel detect any identified Red Flags, such personnel shall all appropriate steps to respond and mitigate

identity theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to the following examples:

b. Continue to monitor an account for evidence of Identity theft;

c. Contact the student/employee;

d. Change any passwords or other security devices that permit access to accounts;

e. Not open a new account;

f. Close an existing account;

g. Reopen an account with a new number;

h. Notify law enforcement; or

i. Determine that no response is warranted under the particular circumstances.

11. Staff Training and Reporting. College employees responsible for implementing the Program shall be trained under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Employees are expected to notify College personnel in accordance with the procedures set forth in the College's Policy Against Fraudulent, Unethical, Illegal, and Other Dishonest Acts (Policy 6Hx28:1-10), if applicable, once they become aware of an incident of identity theft. At least annually or as otherwise requested by the Program Administrator, the Financial Information Security Plan Committee shall report to the Program Administrator through the College Operations Council on compliance with this Program. The report should address such issues as policy and procedures effectiveness in addressing the risk of identity theft in connection with covered accounts, service provider arrangements, and significant incidents involving identity theft and management's response, and recommendations for changes to the Program (see Program Administration and Maintenance section).

12. Oversight of Service Provider Arrangements. In the event the College engages a service provider to perform an activity in connection with one or more accounts, the College will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

a. Require, by contract, that service providers have such policies and procedures in place; and

b. Require, by contract, that service providers review the College's Program and report any Red Flags to the Program Administrator.

13. In addition, the College will require all persons with any specific questions regarding their covered accounts to contact service providers directly.

1[2] "Pretext calling" occurs when an individual improperly obtains personal information of College customers so as to be able to commit identity theft. It is accomplished by contacting the College, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the College to release customer-identifying information.

Procedure History:

Adopted 6-20-06; Formerly 6Hx28:06-30

Date of Last Procedure Review: 06-20-2006