ARTICLE XI: POLICIES FOR THE RELEASE OF INFORMATION
Section 1. Right to Privacy Protocols

Policy 1.4:Financial Information Security Program
Issued: May 22, 2003

I. PURPOSE

The Gramm-Leach-Bliley Act (GLBA) and the implementing Rule on Standards for Safeguarding Consumer Information issued by the Federal Trade Commission, mandate that financial institutions develop, implement, and maintain a security program that safeguards nonpublic personal information handled by the institution. To the extent that Chicago State University, an educational institution, engages in GLBA covered financial services, the University establishes this Financial Information Security Program to comply with the GLB Act and the Safeguards Rule. This Financial Information Security Program is a comprehensive program of policies and procedures designed to: (1) ensure the security and confidentiality of nonpublic customer personal information, (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

II. SCOPE OF PROGRAM

This Financial Information Security Program applies to any record containing nonpublic personal information handled or maintained by or on behalf of Chicago State University ("University") or its affiliates. Nonpublic personal information means any information, whether in paper, electronic or other form: (1) a student or other third party provides in order to obtain a financial service from the University; (2) about a student or other third party resulting from any transaction involving a financial product or service between the University and the student or third party; or (3) the University otherwise obtained about a student or third party in connection with providing a financial service to that consumer. The University units covered under the Program are the Bursar's Office, Financial Aid, Information Technology and the Registrar's Office.

III. DEFINITIONS

Covered data and information for purposes of this Program means all personally identifiable financial information required to be protected under the GLBA. Covered data includes information obtained from a student in the course of offering a financial product or serve, or such information provided to the University from another institution.

Financial Service includes such activities as the lending of money; investing for others; providing or underwriting insurance; giving financial, investment or economic advisory services; marketing securities and the like.

Nonpublic personal information means (1) personally identifiable financial information; and (2) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived from using any personally identifiable financial information that is not publicly available.

Personally identifiable financial information means any information: (1) a student or other third party provides in order to

---

B. Identification and Assessment of Risks

The Information Security Program will identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. Currently, the University employs various University and departmental policies, guidelines, standards and practices relating to the privacy and security of confidential or personal information, including student records and student financial information. The directors of covered units will evaluate the effectiveness of such measures. The directors will submit assessment reports to the Program Coordinator, as determined by the Program Coordinator but no less than annually. Risk assessment will include consideration of risks in each of the following areas:

1. Employee Training and Management
   The directors of covered units will ensure that access to covered data is limited to those employees who require the data as part of their essential job duties. The directors will provide security and privacy awareness training to new and current employees that are appropriate for the department and the covered information available. At a minimum, training should address the importance of maintaining information confidentiality and appropriate methods for protecting the covered information. All employees with access to covered data will enter confidentiality agreements with the University.

2. Information Systems
   The directors of covered units, in consultation with the Information Technology Department, will assess the risks to nonpublic financial information associated with the University's information systems. Assessments will include the adequacy of network and software design, information processing, storage, transmission and disposal. Safeguards providing physical security of covered data have been implemented, including the usage of appropriate information storage, transmission and disposal mechanisms. The directors and Program Coordinator will take reasonable steps consistent with current technological developments to ensure that all covered data is secure.

3. Managing System Failures
   The Office of Information Technology has developed written policies and procedures for detecting any actual or attempted attacks on the University's systems. Consistent with the provisions of the Information Technology Disaster Discovery Plan, the Program Coordinator will evaluate procedures for and methods of detecting, preventing and responding to attacks, intrusions, or other system failures. Reasonable and appropriate measures will be taken to safeguard covered data.

C. Design and Implementation of Safeguards

The University will design and implement information safeguards to control the risks identified through risk assessments. The directors of covered units and the Program Coordinator will regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

D. Oversight of Service Providers

Chicago State University shall take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the covered customer information at issue. By contract, service providers will be required to implement and maintain such safeguards. Pursuant to University practice, the Office of Labor and Legal Affairs will review all contracts with third-party service providers, and will determine that the appropriate terms and provisions safeguarding covered information are included. Any deviation from these standard provisions will required the approval of the Office of Labor and Legal Affairs. Contracts entered into prior to June 24, 2002 are not required to include Safeguards Rule provisions until May 24, 2004.

E. Program Maintenance

This Financial Information Security Program will be subject to periodic review and adjustment. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the Program Coordinator. The Program Coordinator, in consultation with the directors of covered units and the Office of Labor and Legal Affairs, will review the standards set forth in this Security Program and recommend updates and revisions as needed. Adjustments will be made based on: (1) the results of the testing and monitoring required by Section IV; (2) any material changes to the operations or business arrangements; or (3) any other circumstances that

may have a material impact on the University's Financial Information Security Program. The directors of covered units will submit safeguard evaluation reports to the Program Coordinator annually. The Program Coordinator will submit a summary report to the Compliance Officer and the Office of Labor and Legal Affairs annually.

V. UNIVERSITY POLICIES AND PROCEDURES

The University has adopted comprehensive policies, guidelines and procedures relating to information security and privacy. The Financial Information Security Program incorporates by reference the University's policies and procedures enumerated below and are in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

Information Technology Policies

1. Data Security Plan
   http://www.csu.edu/IS/Policy/DataSecurityPlan.pdf

2. Systems And Quality Assurance Plan
   http://www.csu.edu/IS/Policy/systemandquaility.pdf

3. Computer Use Policy
   http://www.csu.edu/IS/Policy/csucomputingpolicy.pdf

4. Rules of Acceptable Use
   http://www.csu.edu/IS/Policy/acceptuse.pdf

5. Disaster Discovery Plan
   [Available in the Office of Information Technology]

Student Affairs Division Policies
[Student Handbook http://www.csu.edu/DOSA/stuhnk.pdf]

6. Policy on Student Confidentiality (p. 53)

7. Computer & Information Security Policy (p. 54)

8. Rights of All Students (p. 54)

Department of Human Resources
[Available in the Office of Human Resources]

9. Confidential Information Policy

10. Criminal Background Investigation Policy

VI. EFFECTIVE DATE

This Financial Information Security Program is effective May 23, 2003.

Filename: Article XI-Section 1-Policy 1.4.doc
Directory: A:
Template: C:\Documents and Settings\delonix\Application Data\Microsoft\Templates\Normal.dot
Title: ARTICLE II: EMPLOYMENT PRACTICES
Subject:
Author: Chicago State University
Keywords:
Comments:
Creation Date: 10/28/2003 5:00 PM
Change Number: 2
Last Saved On: 10/28/2003 5:00 PM
Last Saved By: Chicago State University
Total Editing Time: 1 Minute
Last Printed On: 10/30/2003 1:46 PM
As of Last Complete Printing
Number of Pages: 6
Number of Words: 1,829 (approx.)
Number of Characters: 10,428 (approx.)