Clark University Financial Information Security Plan

1) Purpose:

- In accordance with The Financial Services Modernization Act of 1999, also known as the Gramm Leach Biley Act, and to protect the financial information of our students, faculty, and staff, Clark University has adopted this Financial Information Security Plan. The goal of this document is to outline the measures we will take to comply with this Act, and to assure an ongoing review mechanism to address requests to meet future privacy needs. The Executive Vice President shall serve as the Coordinator of the Plan, and will be assisted by the Vice President for Information Technology, the Controller, and the Registrar, as well as other University Officers as needed.

2) Objectives:

- We will strive to ensure the security and confidentiality of all student and other customer financial records and information. This information will be safeguarded so as to protect to the extent possible any unauthorized access to, or use of, such records in a manner which could cause substantial harm or inconvenience to any customer. We will also protect against any anticipated threats to the security or integrity of this financial information.

3) Risk Assessment: The University will assess the risk to customer financial information from each of the following:

- Unauthorized access to data through software applications
- Unauthorized use of other users' accounts and passwords
- Unauthorized viewing of printed data or computer displayed financial data
- Improper storage of printed financial data
- Unprotected documentation usable by intruders to access data
- Improper destruction of printed financial material

4) Specific Information Security Plans:

- No financial information will be collected by any department of the university which is not necessary for the effective functioning of that Department.
- Printed copies of customer financial information will be shredded when its usage is completed.
- No printed financial information is to be kept in unlocked storage areas. The Physical Plant Department has been instructed to install needed locks and other security devices on a priority basis.
- Printed copies of customer financial information are not to be left on desks when such work areas are unattended.
- Key control of all locked areas will be maintained by the Physical Plant staff, with the cooperation of the University Police and all user departments. All keys must be turned in to
the Director of Human Resources upon separation from the University.

- Computer work stations used to display customer financial information are not to be left unattended with that information displayed. Users of such information are to log off when they are away from their workstation for any significant period of time.

- Passwords are to be utilized, and kept confidential, at all times. These will be controlled by the Department of Information Technology Services.

- Disciplinary measures, up to and including termination, may be imposed for breaches to customer information security.

- Information Technology Services has determined that moving away from the use of Social Security numbers as student identifiers will assist in the protection of customer financial information, and will be doing so.

- All staff utilizing customer financial information (both existing and new hires) will be given a copy of this plan, and asked to signify their acceptance of its provisions.

- All service providers to the University with access to student financial information will be required to implement and maintain safeguards to these data. All existing contracts with such providers shall be modified to include safeguarding requirements no later than May 24, 2004. All new contracts will include these requirements.

- The University will remain in full compliance with the Family Educational Rights and Privacy Act (FERPA)

- The University will continually evaluate and, where necessary, amend this Plan to ensure that customer financial information is protected. This testing will include regular evaluation of the effectiveness of the safeguards put into place, and the key controls, systems, and procedures.

### The Gramm-Leach Bliley Act (GLBA) Information Security Plan

**Purpose:** The Gramm-Leach-Bliley Act, also known as the Financial Modernization Act of 1999, establishes the minimum standards to protect all consumers' personal financial information. This Act includes the Financial Privacy Rule which governs the collection and disclosure of customer's personal financial information by financial institutions and the Safeguard Rule which requires all financial institutions to design, implement, and maintain safeguards to protect customer information.

**Reason for Policy:** In order to ensure the security and confidentiality of private information and data, and to comply with GLB, the University adopted this Information Security Program (GLB) for certain highly critical and private financial and related information. This security program applies to customer financial information ("covered data") the University receives in the course of business as required by GLB, as well as other confidential financial information the University has voluntarily chosen as a matter of policy to include within its scope. This document describes many of the activities the University has established to maintain covered data according to legal and University requirements. This Information Security Program document is designed to provide an outline of the safeguards that apply to this information.

**Entities Affected by this Policy:** Any office or department on campus that either collects, maintains, or has access to records containing protected personal (non-public) financial information for students, faculty, or staff, including but not limited to:

- Admissions Office
- Business and Financial Services
- Business Manager/One Card Office
- COPACE
- Financial Assistance Office
The following is a list of third party servicers who may maintain records with protected personal (non-public) financial information for students, faculty or staff:

- ADP
- ECSI
- Tuition Management Systems (TMS)
- Collection Agencies - Windham Professionals, Delta Management
- Payment Gateway Providers – Touchnet, Harris, PayPal, Authnet Gateway

**Who Should Read this Policy:** All persons who have access to the protected data, including:

- Administrative and faculty department heads
- Every employee that accesses handles or maintains Clark University records (electronic, paper or other form) containing non-public financial information about a constituent who has a relationship with the University. Clark University employees include full-, part-time and hourly staff members as well as student workers who access, handle or maintain records, particularly in the Business & Financial Services area (including the offices of the controller, business manager, cashier, payroll, accounts payable, and student accounts), Financial Assistance Office, University Advancement (including fundraising and alumni affairs offices), Admissions, Office of Intercultural Affairs, GSOM, COPACE and Athletics. Employees who contract with service providers (third party vendors) who, in the ordinary course of University business, are provided access to covered data. Service providers may include, but are not limited to, banks and financial institutions, businesses retained to transport and dispose of covered data, data analysis firms, collection agencies and payment gateway providers.

**Overview:** Many financial institutions collect personal information from their customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories and social security numbers. GLB requires financial institutions, which includes colleges and universities, to ensure the security and confidentiality of this type of information, whether it is paper, electronic or some other type of format. The GLBA also requires the University to develop, implement and maintain a comprehensive Information Security Program containing the administrative, technical and physical safeguards that are appropriate based upon the University's size, complexity and the nature of its activities. This Information Security Program has five components:

- Designating an employee or office responsible for coordinating the program
- Conducting risk assessments to identify reasonably foreseeable security and privacy risks
- Ensuring that safeguards are employed to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored
- Overseeing service providers
- Maintaining and adjusting this Information Security Program based upon the results of testing and monitoring conducted as well as changes in operations or operating systems.

**Definitions:**

A *Financial institution* is as a company that offers financial products or services to individuals, like
loans, financial or investment advice or insurance.

A customer is consumer who has developed an ongoing relationship with a financial institution. In general, if the relationship between the financial institution and the individual is significant or long-term, the individual is a customer of the financial institution.

A consumer is an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family or household purposes, and also means the legal representative of such an individual.

Covered data includes information obtained from a constituent with whom the University has a relationship in the course of offering a financial product or service or conducting fundraising activities; or such information provided to the University from another institution. Constituents include students, employees, service providers, alumni, parents and friends (friends are defined as prospective donors or volunteers who do not have other relationships to the University).

A Financial product or service includes offering student loans, receiving income tax information from a current or prospective student's parents as a part of a financial aid application, offering credit or interest bearing loans, and other miscellaneous financial services. Examples of financial information relating to such products or services include bank account numbers, credit card numbers, income and credit histories, social security numbers and wills and other testamentary documents.

Service Providers refer to all third parties who, in the ordinary course of University business, are provided access to covered data. Service providers may include businesses retained to transport and dispose of covered data, collection agencies, loan servicers, collection agencies, and payment gateway providers.

Procedures:

Risk Assessment

The Information Security Program will identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. Risk assessments will include consideration of risks in each area that has access to covered information. Risk assessments will include, but not be limited to, consideration of employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal; and systems for detecting, preventing, and responding to attacks, intrusions, or other system failures.

The Coordinator will work with all relevant areas to carry out comprehensive risk assessments. Risk assessments will include system-wide risks, as well as risks unique to each area with covered data. The Coordinator will ensure that risk assessments are conducted at least annually and more frequently where required. The Coordinator will work with the CIO to identify a responsible party from the Clark University Information Technology Department to conduct the system-wide risk assessment. The Coordinator may identify a responsible party in each unit with access to covered data to conduct the risk assessment, or employ other reasonable means to identify risks to the security, confidentiality and integrity of covered data in each area of the University with covered data.
Information Safeguards and Monitoring

The Information Security Program will verify that information safeguards are designed and implemented to control the risks identified in a risk assessments. The Coordinator will work with departments to ensure that reasonable safeguards and monitoring are implemented and cover each unit that has access to covered data. Such safeguards and monitoring will include the following:

**Employee Management and Training**

Safeguards for security will include management and training of those individuals with authorized access to covered data. The Coordinator will, working with other department heads, help to identify categories of employees or others who have access to covered data. The responsibility for employee training will reside with various individuals as deemed appropriate by the policy coordinator and the Information Security Officer.

**Information Systems**

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal. Network and software systems will be reasonably designed to limit the risk of unauthorized access to covered data. This may include designing limitations to access, and maintaining appropriate screening programs to detect computer hackers and viruses and implementing security patches.

Safeguards for information processing, storage, transmission, retrieval and disposal may include:

- Requiring that financial information be collected only by departments which it is necessary for the effective functioning of that department.
- Requiring electronic covered data be entered into a secure, password-protected system
- Using secure connections to transmit data outside the University
- Using secure servers
- Ensuring covered data is not stored on transportable media (floppy drives, zip drives, etc)
- Permanently erasing covered data from computers, diskettes, magnetic tapes, hard drives, or other electronic media before re-selling, transferring, recycling, or disposing of them
- Storing physical records in a secure area and limiting access to that area
- Disposing of outdated records under a document disposal policy that includes shredding confidential paper records before disposal; insuring third-party providers provide certification of secure method of shredding and/or disposal
- Requiring that printed financial information be kept in locked storage areas and not left on desks when work areas are unattended.
- Ensuring that computer work stations used to access financial information not be left unattended with that information displayed. Users of such information are required to log off when they are away from their workstation.
- Ensuring that computers with covered data are identified and procedures followed to insure the security of that data during its life cycle in the University's possession or control.

**Monitoring and Testing**

Monitoring procedures will be used to regularly test and monitor the effectiveness of information security safeguards to ensure that safeguards are being followed, and to swiftly detect and correct breakdowns in security.

**Service Providers**

In the course of business, the University may from time to time appropriately share covered data
with third parties. Such activities may include collection activities, loan servicing, payment plan providers, credit card processors, transmission of documents, destruction of documents or equipment, or other similar services. This Information Security Program will ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.

**Responsible Organization/Party:** The Executive Vice President shall serve as the Coordinator of the policy and will be assisted by the Chief Information Officer, the Controller, as well as other University Officers as needed.

**Enforcement:** The University's Information Security Officer will oversee enforcement of the policy, including the responsibility of notifying Department Heads about changes to the policy. Additionally this individual will investigate any reported violations of this policy, lead investigations about indentified security breaches and may terminate access to protected information of any users who fail to comply with the policy.

**Related Policies, Laws and Resources:** The Federal Trade Commission (FTC) has stated that colleges and universities are considered in compliance with the privacy provisions of GLB if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). The University has adopted comprehensive policies, standards, and guidelines relating to information security, including FERPA. Other related polices (www.clarku.edu) are incorporated by reference into this Information Security Plan, and include:

**Policies**

- FERPA
- PCI
- Red Flag
- Appropriate Use of Clark's Information Technology System
- Data Access Policy
- Network-Related Policies

Date of Creation: March 3, 2009
Date of Revision: March 3, 2009