SWARTHMORE COLLEGE
Gramm-Leach-Bliley
Information Security Plan

Background

The Gramm-Leach-Bliley Act of 2000 (GLB) mandates that financial institutions must take steps to safeguard the security and confidentiality of customer information. The Federal Trade Commission (FTC) ruled that GLB applies to institutions of higher education. Compliance with GLB involves compliance with 1/ the **privacy** provisions of the act and 2/ provisions regarding the **safeguarding** of customer information. The FTC has said that colleges are deemed in compliance with the privacy provisions of GLB if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). With respect to the second area, GLB specifies new requirements for colleges to safeguard non-public customer information, such as family financial information and social security and identification numbers, by having an institutional security program and security plans in specific offices of the college that handle such information.

Designated Security Program Officers

The designated GLB Security Program Officers for Swarthmore College are Suzanne P. Welsh, Vice President for Finance and Treasurer, and Martin Warner, Registrar. All correspondence and inquiries about the Swarthmore College Information Security Plan should be directed to one of these Officers.

Customer Information

For purposes of FERPA and GLB, the College considers students, employees, and alumni or any other third party engaged in a financial transaction with Swarthmore College as "customers". Customer information that must be safeguarded is "any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form." It includes financial information, academic and employment information, and other private paper and electronic records.

Privacy Provisions

With respect to the privacy provisions of the GLB Act, Swarthmore College is in compliance with FERPA. Directory information (for example, name, address, enrollment at the college and degree information), the list of which is published

yearly in the Student Handbook, is considered public (unless a student has requested otherwise in writing). All non-directory information is restricted or confidential, what GLB calls "non-public." Under FERPA, restricted information (for example, academic or financial records) is released outside the college only with the student's written consent. Designated school officials, including faculty, key employees and occasionally outside service providers, have access to restricted, "non-public" information on a need-to-know basis only. Confidential information (for example, a faculty member's or dean's private notes) is even more protected than restricted information, and released only in certain unusual circumstances as outlined in FERPA. Although FERPA if narrowly construed only applies to enrolled students and past students, in compliance with GLB and long standing good practice, the College extends FERPA privacy protections to all customers of the college.

The Registrar's Office will provide guidance in complying with all FERPA privacy regulations. In addition, the College also complies with HIPAA (Health Insurance Portability and Accountability Act of 1996) with the Health Center and Human Resources providing guidance on this Act. Each department is responsible for securing customer information in accordance with all privacy guidelines.

Security Provisions

With respect to the safeguarding provisions of the GLB Act, the Swarthmore College GLB Information Security Plan herein is designed to ensure the security, integrity, and confidentiality of non-public customer information, protecting it against anticipated threats, and guarding it against unauthorized access or use. Covered under the Plan are administrative, technical, and physical safeguards used in the collection, distribution, processing, protection, storage, use, transmission, handling, or disposal of non-public customer information. The Plan covers actions by both employees of the College and outside service providers.

The policies incorporated in this document apply to all College departments. In addition, in the case that individual departments may have additional security provisions, they will maintain written documentation of these and will make them available to the Security Program Officers. For example, the information technology department will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information.

The College security policies for departments include the elements described in the following sections.

Physical Safeguards

The College uses direct personal control or direct supervision to control access to and handling of all non-public customer information when an office is open. Whether the information is stored in paper form or any electronically accessible format, departmental non-public information is maintained, stored, transmitted and otherwise handled under the direct personal control of an authorized employee of the College.

Departmental non-public information is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security. Conversations concerning non-public information are held in private. Papers with non-public information are mailed via official campus mail, US mail, or private mail carrier. Departments are encouraged to password-protect electronic files of non-public information when transmitting electronically. When best practices permit the disposal of non-public information, it is destroyed; paper containing such information is routinely shredded or otherwise destroyed.

Confidential material is kept secure. Most offices have locked windows and locked doors with restricted access. For those that do not, materials are kept in locked filing cabinets or other locked storage areas. When offices are open, confidential information is kept out of sight from visitors, and computer screens are not visible to visitors. Offices and/or computers are locked when the office will be vacant for an extended length of time.

Key access is limited to authorized College employees only, in the context of College key control governing the distribution of keys. College Public Safety further ensures the security of offices after hours.

Departmental offsite storage and information processing generally conforms to the same practices as onsite storage, and is safeguarded under the provisions for outside service providers, as described below.

Technical Safeguards

The College relies on the Information Technology Services Department to provide network security and administrative software password access security according to industry standards in order to protect non-public customer information that is accessed electronically but stored outside of a department.

Departmental desktop computers and other electronic devices storing non-public customer information are protected by physical safeguards.

The Information Technology Services Department maintains its own written security policy which is incorporated with the overall College policy. This is included as Appendix A.

Employee Management and Training

All College employees, including part-time and temporary employees, and volunteers are given specific training by their supervisors about issues of security of sensitive and confidential material used in their respective offices. Employees are held accountable to know that although they have access to non-public information in order to perform their duties for the College, they are not permitted to access it for unapproved purposes or disclose it to unauthorized persons. The Employee Handbook, which is provided to all employees, states that violation of security policies could result in termination of employment or legal action, or both.

Outside Service Providers

Each area will assure that third party service providers are required to maintain appropriate safeguards for nonpublic information to which they have access. Contracts with service providers, who within their contracts have access to Swarthmore College non-public customer information, shall include the following provisions as appropriate:

Explicit acknowledgment that the contract allows the contract partner access to confidential information;

Specific definition of the confidential information being provided;

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

Guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;

Guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;

Provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;

Stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;

Stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Swarthmore College to immediately terminate the contract without penalty;

Provision allowing auditing of the contract partners' compliance with the contract safeguard requirements;

Provision ensuring that the contract's protective requirements shall survive any termination agreement.

Reassessment of Plan

This Plan and any other individual departmental policies are reviewed at least annually and adjusted as needed. The GLB Security Program Officers circulate this policy to each department and request a reassessment. The annual reviews include identification and assessment of internal and external risks to the security, integrity, and confidentiality of non-public customer information, including review of outside contractors and their contracts to ensure that proper safeguards are in place.

APPENDIX A
SWARTHMORE INFORMATION TECHNOLOGY SERVICES
SECURITY PROGRAM 2005

Background:

Protecting customer information is a shared responsibility between institutional offices and the Information Technology Services staff. Institutional offices are directed to develop a written security policy that details the policies and processes in place in each relevant area where a risk to customer information is evident. Those offices include: Alumni and Development, Registrar's Office, Financial Aid Office, Admissions Office, Human Resources, and Student Accounts Receivable Office, Health Center, and Residence Life.

Information Technology Services (ITS) will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information. This document is an outline of ITS practices in place that protect electronic information.

ITS Practices/Policies:

Network security, including firewall technology, has been implemented to protect administrative servers and departmental workstations from unauthorized access through the Internet. Staff in administrative and faculty offices connect to secured computers on the campus network. Off campus access to this subnet is provided through a secure Virtual Private Network (VPN) complete with encryption and an additional layer of password security.

Desktop computers in administrative offices provide the most vulnerable point of access to administrative systems. Desktop computers are physically locked to desktops and are behind a firewall.

Nightly backups of important documents and files secures information from loss.

Printed reports containing confidential and sensitive data are secured within offices or behind locked doors in the central computer room. Reports that are no longer needed,

containing confidential and/or sensitive data, are shredded or stored securely until they are shredded.

In addition to network and physical security, the logical security plans are a fundamental layer of protection. These plans are the key to protecting administrative information and describe the procedures by which system privileges are granted, passwords maintained, security monitored and issues communicated.

System privileges are authorized by the Department Head or designated *Department security manager* and centrally assigned by ITS System Administrators in the Database Services group. Department Heads include the Dean of Admissions, Registrar, Controller, Associate VP for Human Resources, Director of Financial Aid, etc.

Faculty and staff granted access to institutional data may do so only to conduct College business. In this regard, employees must:

*Respect the confidentiality and privacy of individuals whose records they access
* Observe ethical restrictions that apply to the data to which they have access
*Abide by applicable laws or policies with respect to access, use, or disclosure of information

Employees may not:

*Disclose data to others, except as required by their job responsibilities
*Use data for their own personal gain, nor for the gain or profit of others
*Access data to satisfy their personal curiosity

Employees and students who violate this policy are subject to the investigative and disciplinary procedures of the College. The Office of the Dean of Students handles complaints against students. The Provost handles complaints against faculty. Complaints against staff and administrators are handled through Supervisors or Human Resources.

Definition of Administrative Information

Administrative information is any data related to the business of the College including, but not limited to, financial, personnel, student, alumni, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside. *Administrative information* does not include library holdings or instructional notes unless they contain information that relates to a business function.

The College recognizes *administrative information* as a College resource requiring proper management in order to permit effective planning and decision-making and to conduct business in a timely and effective manner. Employees are charged with safeguarding the integrity, accuracy, and confidentiality of this information as part of the condition of employment.

Access to administrative systems is granted based on the employee's need to use specific data, as defined by job duties, and subject to appropriate approval. As such, this access cannot be shared, transferred or delegated. Failure to protect these resources may result in disciplinary measures being taken against the employee, up to and including termination.

Requests for release of administrative information are referred to the office responsible for maintaining those data. The College retains ownership of all administrative information created or modified by its employees as part of their job functions. Administrative information is categorized into three levels:

Confidential information requires a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration or destruction of the data. This includes information whose improper use or disclosure could adversely affect the ability of the College to accomplish its mission as well as records about individuals requiring protection under the *Family Educational Rights and Privacy Act of 1974* (FERPA).

Confidential information includes, for example, student financial aid information, salary and benefits information, alumni gifts and student grades.

Sensitive information requires some level of protection because its unauthorized disclosure, alteration, or destruction might cause damage to the College. It is assumed that all administrative output from the administrative database is classified as sensitive unless otherwise indicated.

Sensitive information includes, for example, class lists, contract data, and vendor data information.

Public Information can be made generally available both within and beyond the College. It should be understood that any information that is widely disseminated within the campus community is potentially available to the public at large.

Public information includes, for example, telephone directory information.

Employee Information

All aspects of personnel records are confidential. Directory information for faculty and staff as published in the *Swarthmore College Telephone Directory* is public. Directory information may include some or all of the following: name, home telephone, spouse/partner name, department, position title, campus address, campus phone and email address. All data maintained in the published Telephone Directory is also available on-line from off campus locations. Faculty and staff may request that this data be classified as confidential. <u>All other employee related data, especially that which is available to users outside Human Resources such as social security number and birth date, must be vigilantly safeguarded and treated as confidential.</u>

Family Educational Rights and Privacy Act (FERPA)

The *Family Educational Rights and Privacy Act* (FERPA) of 1974 govern all information about students, current and former, maintained by Swarthmore College. FERPA generally requires that Swarthmore College have the student's written permission to release any information from their records except certain types of "directory information."

Student "Directory Information", as defined by FERPA

Certain information, classified as "directory information", is available for public consumption unless the student specifically directs that it be withheld. The student may direct the Office of the Dean of Students not to disclose such information. Former students may contact Alumni Relations.

Public directory information as defined by the Act includes: student's name, address, telephone number, date and place of birth, major field of study, participation in officially organized activities and sports, dates of attendance, degree and awards received, and the most recent previous educational institution attended.

Security process of the central administrative database (Banner)

Assigning privileges:

Department security managers (department heads or their designee) are responsible for authorizing system access to Banner. ITS System Administrators in Database Services will assign that access.

A similar process exists for authorizing access to the course management system (Blackboard), electronic mail and central fileservers.

The *Security Request Form* for Banner access must be completed by the Department security manager to authorize, modify or remove user privileges.

<u>NEW Employee to department</u>:

1. Department Security Manager explains the Security Policy to the new employee and provides a written copy.
2. Department Security Manager emails request to ITS System Administrator attaching the *Security Request Form*.
3. ITS System Administrator creates the login and assigns Security Classes.
4. ITS System Administrator replies to Department Security Manager's original email indicating the security has been established and schedules an appointment with new user.
5. Department Security Manager prints and signs *Security Request* Form.

6. Employee carries signed *Security Request Form* and last page of the Security Policy signed by the user to ITS System Administrator to acquire a password.
7. ITS System Administrator files signed *Security Request Form*
8. Department Security Manager provides training and documentation to employee.
9. Employee must change password upon first login.

Modification and Termination:

ITS should be notified immediately as soon as an employee is terminated. The ITS System Administrator will disable all account access for that employee.

On a daily basis, ITS System Administrators will review reports identifying failed login attempts, including unsuccessful attempts by individuals to access portions of the system to which they are not authorized. After five consecutive failed login attempts, accounts are automatically deactivated. ITS will immediately notify the Department security manager and other appropriate College officials if it appears security has been breached.

Ideally, at the end of each payroll period, Human Resources will report to the ITS System Administrators new hires, transfers and terminations.

Effective July 1, 2005, on a quarterly schedule, ITS will provide Department security managers with a list of all system privileges in their area. Department security managers will be required to review and approve.

Passwords

Administrative information is protected through the vigilant use of user-defined passwords.

Passwords must be:

*Changed by the user on-line every ninety days
*Changed by the user no more frequently than every five days
*Consist of both letters and numbers
*Six characters in length, minimum
*Significantly different from prior passwords

Individuals are expected to protect passwords from disclosure. Every individual must have a unique user login.

Responsibility of Institutional Offices

Department Security Manager

The department head of each administrative office must assign a Department security manager and an alternate who is responsible to authorize and monitor access to the administrative system.

A *Security Request Form* must be completed for each individual who is provided access to the administrative system. This same form must be completed to modify or remove access. It is just as important to remove access to the administrative system, as it is to authorize access to the administrative system.

On a quarterly basis, the Department security manager will be required to review all security authorizations for the department. A report will be produced and distributed by the ITS System Administrators.

Communication to new employees

Department heads or security managers are responsible for discussing this policy with each employee at the time system privileges are issued. Effective, on-going communication of this security policy along with instruction regarding office procedures is the responsibility of each department head.

March, 2005