Goucher College Information Security Program (DRAFT)

A. Purpose

The purpose is to:

1. Define the college's Information Security Program to protect and safeguard college information and data
2. Outline a process to conduct regular information security and privacy risk assessments
3. Outline a process for evaluating and implementing information security safeguards
4. Develop and refine an employee security training program
5. Outline a process to assure ongoing compliance with federal regulations
    - Financial Services Modernization Act of 1999 also known as Gramm Leach Bliley (GLB), 15 U.S.C. § 6801
    - Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g
6. Prepare the college for any future privacy and security regulations

In order to protect college critical information and data, and to comply with federal law, Information Technology and the General Counsel's Office propose certain practices in the college information environment and institutional information security procedures. While these practices mostly affect Information Technology, some of these practices will impact diverse areas of the college, including but not limited to Business Services, Controller's Office, Development and Alumnae/i Affairs, Human Resources, Student Administrative Services, and third party contractors, including food services and the bookstore.

B. Gramm Leach Bliley (GLB) Requirements

The Gramm Leach Bliley (GLB) Act mandates that the institution:

1. Appoint an Information Security Program Coordinator
2. Conduct a risk assessment of likely security and privacy risks
3. Institute a training program for all employees who have access to covered data and information
4. Oversee service providers and contracts
5. Evaluate and adjust the Information Security Program periodically

C. Information Security Program Committee and Coordinator

In order to comply with the Gramm Leach Bliley Act, Information Technology has designated an Information Security Program Coordinator. This individual must work closely with the General Counsel's office, other positions in Information Technology, and all relevant academic and administrative departments throughout the college. The Coordinator is presently the Chief Technology Officer.

The college has established an Information Security Program Committee consisting of the:

1. Bursar
2. Chief Technology Officer
3. College Librarian
4. Controller
5. Coordinator of Access Card System
6. Director of Administrative Computing
7. Director of Computing Services
8. Director of Development Research and Information
9. Director of Financial Aid
10. Director of Human Resources
11. Director of Networking and Telecommunications
12. General Counsel
13. Registrar
14. System Administrators for the college's Windows and UNIX computer servers

The Information Security Program Committee and Coordinator will help the relevant departments of the college identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a safeguards program; and regularly monitor and test the program.

D. Risk Assessment and Safeguards

Goucher College will complete the following tasks to assess security risks and to implement security safeguards:

1. Perform Regular Reviews of Information Technology Security Risks and Security Procedures

Information Technology will conduct a regular review of the college's computer servers, computing systems, and network infrastructure in the following areas:

a. **Fault Management:** Fault management is the set of facilities that enables the detection, isolation and correction of abnormal operation.

b. **Configuration Management:** Configuration management is the set of facilities which records the current configuration, records changes in the configuration and changes network parameters.

c. **Performance Management:** Performance Management is needed to optimize the quality of service. It includes the use of tools to detect changes in the network's performance.

d. **Security Management:** Security Management is the set of facilities that enables the manager to initialize and modify those functions that secure the network from users' unauthorized activities.

e. **Network Administration:** Network Administration verifies that procedures and controls exist to ensure that the system functions effectively and efficiently in all phases of operations and maintenance in order to provide maximum system availability and performance.

f. **Standards:** Management must provide standards for the effective and efficient operation of the end user environment.

g. **Systems and Programming Controls:** Systems and Programming Controls verify that management is exercising proper control over the installation, maintenance, and use of the vendor/user developed software/hardware resident on the enterprise network.

h. **Logical Security:** Logical Security measures need to be implemented to ensure that proper controls are in effect for the security of organization data files and program libraries.

i. **Physical Security:** Physical Security measures need to be implemented to ensure procedures and equipment are in use to provide adequate physical security for the computer equipment, including theft, vandalism, fire detection and prevention, support the requirements of the operation of the system hardware.

j. **Contingency Planning:** Contingency Planning needs to be completed to ensure that an adequate plan exists for the timely and logical recovery of processing operations following some sort of interruption, denial of service, etc.

k. **Communication Security:** Communication Security measures need to be in place to ensure that management has instituted polices and procedures that will protect sensitive data from being changed, intercepted, or unprotected on the Local Area Network.

l. **Training:** Training needs to be planned and implemented to ensure that operators and other technical staff are adequately trained in the effective, secure, and efficient use of system resources.

Information Technology will assure that security procedures are consistent with those practiced at other national liberal arts colleges, as measured by the recommendations and procedures of four advisory groups: The EDUCAUSE Security Institute, the Internet2 security working group, the SANS Top Twenty risks list, and the Federal NIST Computer Security Resource Center.

2. Perform Regular Operating System and Software Updates

Information Technology will install software fixes, patches, and upgrades to correct operating system problems, security issues, and performance concerns. Organizations that fail to install the latest software releases and upgrades are subject to servers that fail because of vulnerability or may be subject to attacks by hackers, viruses, or worms.

3. Perform a Regular Audit of College Computer and Information System Accounts

Information Technology will perform a regular audit of computer accounts to insure that accounts are deleted for individuals who are no longer employed by the college or information system access is changed appropriately when an individual changes their job or job responsibilities.

4. **Perform an Annual Review of the Computer Use Policy**
The Information Technology Advisory Group (ITAG) will review the college's Computer Use Policy (http://www.goucher.edu/it/index.cfm?page_id=40) on an annual basis to determine if changes are needed to the policy.

5. **Perform a Regular Review of the Computer Account Generation Process**
Information Technology will perform a regular review of the process and procedures that are used to create, delete, and modify computer accounts and information system access to data.

6. **Perform a Regular Review of Backup and Recovery Procedures**
Information Technology will conduct a regular review of the college's backup and recovery procedures. The review of backup and recovery procedures will include:
   a. How are Problems or Failures reported?
   b. College Information Systems
   c. Other College Business Systems
   d. E-mail
   e. College Web Site
   f. Other Campus Computing Systems
   g. Telecommunications
   h. Network Infrastructure
   i. Campus Connection to the Internet
   j. Computer Workstations
   k. Equipment Failure
   l. Destruction by Fire
   m. Vandalism / Loss
   n. Inadequate Backup
   o. Power Outage
   p. Environmental problems
   q. Computer Viruses
   r. Security Issues

7. **Perform a Regular Review of the Campus Use of Social Security Numbers**
While the college has discontinued usage of social security numbers as student identifiers, one of the largest security risks may be possible non-standard practices concerning social security numbers (e.g. continued reliance by some college employees on the use of social security numbers). Social security numbers are considered protected information under both GLB and

FERPA. By necessity, student social security numbers still remain in the college's information systems. The college will perform a regular review to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. This assessment will cover college employees as well as subcontractors such as the bookstore and food services.

8. Develop a Records Management Policy and Perform Regular Reviews

The college will develop a Records Management Policy for the continual, economical, and efficient management of its records. The Records Management Policy is intended to:

- Guide departments in their legal obligations with record retention and disposal
- Standardize the record keeping practices at the institution
- Encourage the proper disposal of records for the sake of space
- Allow the college to meet its legal obligations with retention, disposal and proper handling of records

9. Perform Departmental Security and Data Audits

The Information Security Program Committee will work with all relevant areas of the college to identify potential and actual risks to security and privacy of information. Each relevant department will conduct a regular data security review with guidance from the Information Security Program Committee. The relevant departments will conduct a review of procedures, incidents, and responses. Relevant college departments will develop and maintain a data handbook, listing those persons or offices responsible for each covered data field in relevant software systems (Financial, Student Administration, Financial Aid, Alumni/Development, etc.). Information Technology and the relevant departments will conduct ongoing audits of activity and will report any significant questionable activities.

10. Conduct regular reviews of Security Incidents

Information Technology will track the detection, prevention, and responses to security attacks, intrusions, or other systems failures. A regular review will be conducted of the incidents and responses in order to plan future strategies.

11. Complete annual outside audit of Information Technology

Each year, the college is audited by an outside auditing firm. Part of the college's annual audit is the audit of the operations of Information Technology and the college's computing and information systems. The outside auditing firm provides Performance Improvement Opportunities if applicable.

E. Employee Training and Education

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, the Information Security Program Committee in cooperation with the Office of Human Resources and Information Technology will develop training and education programs for all employees who have access to data outlined in the Information Security Program. These employees typically fall into three categories: professionals in information technology who have general access to all college data, custodians of data (those individuals who are responsible for a subsystem of the college's information systems), and those employees who use the data as part of their essential job duties.

F. Oversight of Service Providers and Contracts

GLB requires the college to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Business Services, in cooperation with the General Counsel, will develop and send form letters to all covered contractors requesting assurances of compliance with GLB. While contracts entered into prior to June 24, 2002 are grandfathered until May 2004, the General Counsel will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with GLB.

G. Evaluation and Revision of the Information Security Program

GLB mandates that an institution's Information Security Program be subject to periodic review and adjustment. The most frequent of these reviews will occur within Information Technology. Constantly changing technology and constantly evolving risks necessitates quarterly reviews within Information Technology. Processes in other relevant offices of the college such as data access procedures and the training program should undergo a review on a regular basis. The college's Information Security Program will be reviewed annually in order to assure ongoing compliance with existing and future laws and regulations.

H. Definitions

1. **Covered data and information** for the purpose of this policy includes student financial information required to be protected under GLB. In addition to this coverage which is required by federal law, Goucher College chooses as a matter of policy to also define covered data and information to include any credit card information received in the course of business by the college, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

2. **Student financial information** is information that the college has obtained from a student in the process of offering a financial product or service, or information provided to the college by another financial institution. Offering a financial

product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers, in both paper and electronic format.

I. Acknowledgements and Reference Information

This Information Security Program is adapted in part from:

1. Catholic University of America Office of General Counsel Gramm Leach Bliley (GLB) Web Site (http://counsel.cua.edu/glb/)
2. National Association of College and University Business Officers (NACUBO) Gramm Leach Bliley Act Bulletin and Sample Information Security Plan (http://www.nacubo.org/public_policy/bulletins/2003/04252003.asp)
3. National Association of College and University Attorneys (NACUA) Sample Information Security Plan (http://www.nacua.org/documents/GLBSafeguardsPlan-Public.pdf)
4. Federal Trade Commission Financial Privacy: The Gramm-Leach Bliley Act (http://www.ftc.gov/privacy/glbact/)
5. U.S. Department of Education Family Educational Rights and Privacy Act (FERPA) (http://www.ed.gov/offices/OII/fpco/ferpa/)