GOUCHER | college

Written Information Security Program

I. INTRODUCTION

Goucher College developed this Written Information Security Program (the "Program") to protect Confidential Data, as that term is defined below, found in records and systems owned and/or operated by the College. This Program is intended as a comprehensive set of guidelines and policies that have been implemented in compliance with federal and state law, including the financial customer information security provisions of the federal Gramm-Leach-Bliley Act ("GLB") [15 USC 6801(b) and 6805(b)(2)] and by the Federal Trade Commission [16 CFR Part 314]; and the Maryland Personal Information Protection Act, Md. Code Ann. Comm. Law 14-3504.

This Program will be periodically reviewed and amended as necessary to protect Confidential Data.

II. PURPOSE

The purposes of this document are to:

- Establish a Program for Goucher College designed to protect the Confidential Data of students, alumnae, faculty, and other employees of the College;
- Establish employee responsibilities for safeguarding Confidential Data; and
- Outline procedures to implement and administer this Program, including administrative, technical and physical safeguards.

For the purposes of this Program, Goucher College employees include all faculty, administrative staff, union staff, contract and temporary workers, student employees and hired consultants.

A. **Personal Information,** as used in this Program, means the first name or first initial and last name of a person when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable, in combination with any one or more of the following:
   1. Social Security number;
   2. Driver's license number; or
   3. A financial account number, including a credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account;
   4. An Individual Taxpayer Identification Number.

NOTE: For purposes of this policy, Personal Information does not include Goucher assigned student identification numbers, although such information should be treated as other student information and is protected under the Family Educational Rights and Privacy Act (FERPA).

B. Nonpublic Financial Information is financial information about a constituent of the College (student, employee, parent, alumni, donor, etc.), whether in paper, electronic or other form, that is handled or maintained by or on behalf of the College. For these purposes, NFI shall include any information:

1. A constituent provides in order to obtain a financial product or service from the College;
2. About a constituent resulting from any transaction with the College involving a financial product or service; or
3. Otherwise obtained about a constituent in connection with providing a financial product or service to that person.

Examples of NFI include:

1. Information a student provides to you on an application to obtain a student loan, including tax returns;
2. Account balance information, payment history, overdraft history, and credit or debit card purchase information;
3. The fact that an individual is or has been one of your constituents and has obtained a financial product or service from you;
4. Any information that a student provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
5. Any information you collect through an Internet "cookie" (an information collecting device from a web server); and
6. Information from a consumer report.

C. Confidential Data includes Personal Information and Nonpublic Financial Information.

III. RESPONSIBILITIES

A. The General Counsel:

1. Is in charge of maintaining, updating, and implementing this Program.
2. Is responsible for ensuring that all breaches are documented and subsequent responsive actions taken.
3. Maintains records of breaches a file in the office of the General Counsel.
4. In conjunction with the Vice President for Information Technology, reviews incidents of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Confidential data, and, when appropriate, convenes a team of employees to form an incident response task force to determine appropriate responses when a breach occurs.

B. **All employees** are responsible for maintaining the privacy and integrity of Confidential Data and to access, store and maintain records containing Confidential Data in compliance with this Program.

C. **Reporting Attempted or Actual Breaches of Security**

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Confidential Data, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the General Counsel.

D. Risk Assessment

All employees who handle Confidential Data are responsible for identifying, within their own work areas and functions, the reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Confidential Data that could result in unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of such information. Among the foreseeable risks are:

1. Unauthorized access of Confidential data by someone other than the owner of such data
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 hard copy files or reports
9. Unauthorized transfer of Confidential Data through third parties

All employees are responsible for reviewing safeguards within their own work areas and functions to determine their sufficiency to control these risks, and shall bring to the attention of the General Counsel any perceived insufficiency in safeguards.

E. Violations

Any employee who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Confidential Data without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action as determined by the employee's supervisor.

IV. Policies and Procedures for Safeguarding Information

To protect Confidential Data, the following policies and procedures have been developed:

A. Access

1. Only those employees or authorized third parties requiring access to Confidential Data to perform their job duties shall be granted access to Confidential Data, including both physical and electronic records.
2. Upon termination of an employee's employment, the employee's access to computer access passwords shall be immediately terminated. In the case of retirements, retirees are allowed to retain their Goucher email account, but may not retain access to data from the college's computer systems.
3. Upon termination of employment, physical access to documents or other resources containing Confidential Data is immediately prevented.

B. Storage

1. Confidential Data must not be stored on cloud-based storage solutions that are unsupported by the College (including DropBox, Microsoft OneDrive, Apple iCloud, etc.).
2. Members of the Community are strongly discouraged from storing Confidential Data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives). However, if it is necessary to transport Confidential Data electronically, the mobile device containing the data must be encrypted (see below).
3. Paper records containing Confidential Data must be kept in locked files or other areas when not in use, and should not be removed from the premises of the College.
4. Electronic records containing Confidential Data must be stored on secure servers, and should not be stored on laptops or desktop computers. When stored on authorized desktop computers, such files must be password protected.
5. Confidential Data should not be emailed. Instead users should create a secure site on Inside Goucher or in a departmental folder to share data with other users.
6. When it is necessary to remove records containing Confidential Data from campus, employees must safeguard the information. Under no circumstances are documents, electronic devices, or digital media containing Confidential Data to be left unattended in any insecure location.
7. When there is a legitimate need to provide records containing Confidential Data to a third party, electronic records containing such information should be password-protected and encrypted, and paper records marked confidential and securely sealed.

C. Disposition

Destruction of paper and electronic records containing Confidential Data must be carried out in accordance with the Goucher College Records Management Policy, and any other applicable federal, state and local regulations. Shredding, using a cross-cut or strip shredder, should be used for all documents that contain Confidential Data; alternatively the college contracts with a provider to collect and confidentially destroy confidential paper records.

D. Third-party Vendor Relationships

The College exercises diligence in selecting service providers to determine that they are capable of maintaining appropriate safeguards for Confidential Data provided by the College to them. All contracts with service providers who have access to or are provided with Confidential Data must be reviewed and approved by the General Counsel to ensure that the contracts contain the necessary provisions regarding safeguarding Confidential Data.

E. Computer system safeguards

The Vice President for Information Technology will monitor and assess information safeguards on an ongoing basis to determine when enhancements are required. To combat external risk and secure the College network and data that contain Confidential Data, the College has implemented the following safeguards:

1. Secure user authentication protocols
    - Unique strong passwords are required for all user accounts; each employee receives an individual user account.
    - Passwords are required to be changed every 180 days.
    - Server accounts are locked after 5 successive failed password attempts.
    - Computer access passwords are disabled upon employee's termination. In the case of retirements, retirees are allowed to retain their Goucher email account, but the roles to access data from the administrative systems are removed.
    - User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.

2. Secure access control measures
    - Access to specific files or databases containing Confidential Data is limited to those employees who require such access to perform their job duties.
    - Each such employee has been assigned a unique password to obtain access to any file or database that contains Confidential Data needed by the employee to perform his or her job duties.
    - Files containing Confidential Data transmitted outside of the Goucher College network are encrypted.
    - Internal network security audits are performed to all server and computer system logs to discover, to the extent reasonably feasible, possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Confidential Data.
    - All College-owned computers and servers are firewall protected and regularly monitored.
    - Operating system patches and security updates are installed to all servers at least every 30 days.

- Antivirus and anti-malware software is installed and kept updated on all servers and workstations. Virus definition updates are installed on a regular basis.

3. Encryption

   Encryption software will be placed on laptop and desktop computers that contain Confidential Data. This will include computers that belong to the following departments:

   - Admissions
   - Bursar / Billing
   - Business Services
   - Controller's Office and Accounts Payable
   - Counseling Center
   - Finance and Administration
   - Financial Aid
   - General Counsel
   - Health Center
   - Human Resources/Payroll
   - Information Technology
   - Institutional Effectiveness
   - Office for Strategic Initiatives
   - Office of Accessibility Services
   - Office of Advancement
   - President's Office
   - Provost's Office
   - Registrar's Office

F. Training

Appropriate initial and periodic ongoing training is provided to all employees who are subject to policies and procedures adopted within this Program or who otherwise have access to Confidential Data.

G. Policies cross-referenced

The following Goucher College policies provide advice and guidance that relates to this Program:

- FERPA Policy
- Red Flag Policy
- Computer Use Policy

This Written Information Security Program is effective February 1, 2017.