Wellesley College
Written Information Security Program

Introduction and Purpose

Wellesley College developed this Written Information Security Program (the "Program") to protect Personal Information, as that term is defined below, found on records and in systems owned by the College. This Program is intended as a comprehensive set of guidelines and policies that have been implemented in compliance with regulations issued by the Commonwealth of Massachusetts entitled "Standards For The Protection Of Personal Information Of Residents Of The Commonwealth" (201 Code Mass. Regs. 17.00) This Program will be periodically reviewed and amended as necessary to protect Personal Information.

This Program should be read in conjunction with other College record-keeping and privacy policies that are cross-referenced at the end of this Program.

The purposes of this document are to:

- Establish a Program for Wellesley College with policies designed to protect the Personal Information of students, alumnae, faculty, and other employees of the College that is maintained by the College;
- Establish employee responsibilities in safeguarding data containing Personal Information; and
- Outline procedures to implement and administer this Program, including administrative, technical and physical safeguards.

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

Personal Information, as used in this Program, means the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Driver's license number or other state-issued identification card number; or
- Financial account number or credit or debit card number that would permit access to a person's financial account number, with or without any required security code, access code, personal identification number, or password.

Responsibilities

The Information Security Officer (the ISO) is in charge of maintaining, updating, and implementing this Program. The ISO can be contacted at iso@wellesley.edu.

The ISO reviews incidents of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Personal Information, and, when appropriate, convenes a team of employees to form an incident response task force to determine appropriate responses when a breach occurs. The ISO documents all breaches and subsequent responsive actions taken. Records of breaches are retained in a file in the office of the ISO.

All employees and, to the extent relevant, students are responsible for maintaining the privacy and integrity of Personal Information, and are required to access, store and maintain records containing Personal Information in compliance with this Program.

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 Personal Information, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the ISO.

Risk Assessment

In developing this Program, the ISO identified to the extent reasonably feasible the locations of all Personal Information maintained by Wellesley College.

Risk assessment takes into consideration risks in each relevant area of the College's operations, including employee training, compliance with this Program, and means for detecting and preventing security system failures.

The ISO, along with other appropriate employees, has identified and continues to identify the reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Personal Information that could result in unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of such information. Among the foreseeable risks are external hacks, unauthorized access, thefts, inadvertent destruction of records, unintentional authorization of access, property damage from environmental hazards, and misuse of access by employees, students or business associates.

The ISO, along with other appropriate employees, has assessed, and on a continuing basis reviews, the sufficiency of safeguards currently in place to control these risks.

Violations

Any employee or student who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises Personal Information without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, which may include termination in the case of employees and expulsion in the case of students.

Policies and Procedures for Safeguarding Information

To protect Personal Information, the following policies and procedures have been developed that relate to protection, access, storage, transportation, and destruction of records, computer system safeguards, and training.

Access

- Only those employees or authorized third parties requiring access to Personal Information in the regular course of their duties are granted access to Personal Information, including both physical and electronic records.
- Computer access passwords are disabled prior to termination of employment.
- Upon termination of employment, physical access to documents or other resources containing Personal Information is immediately prevented.

Storage

- No Wellesley College employee may store Personal Information on a laptop or on external devices (e.g., flash drives, mobile devices, external hard drives) without express authorization by the ISO, and such authorization requires encryption of data and other appropriate safeguards.
- Paper records containing Personal Information must be kept in locked files or other areas when not in use, and may not be removed from the premises of the College, without the express permission of the ISO.
- Electronic records containing Personal Information must be stored on secure servers, and, when stored on authorized desktop computers, must be password protected.

Removing records from campus

- When it is necessary to remove records containing Personal Information off campus, employees must safeguard the information. Under no circumstances are documents, electronic devices, or digital media containing Personal Information to be left unattended in any insecure location.
- When there is a legitimate need to provide records containing Personal Information to a third party, electronic records are password-protected and encrypted, and paper records are marked confidential and securely sealed.
- Wellesley College takes all reasonable steps to select service providers that are capable of maintaining appropriate security measures to protect Personal Information as required by 201 CMR 17.00.

Disposition

- Destruction of paper and electronic records must be carried out in accordance with the Wellesley College Records Management Policy, Chapter 93I of the Massachusetts General Laws, and any other applicable federal, state and local regulations.

Third-party vendor relationships

The College exercises appropriate diligence in selecting service providers to determine that they are capable of maintaining appropriate safeguards for Personal Information provided by the College to them. The primary budget holder for each department is responsible for determining those third parties providing services to the College that have access to Personal Information. All relevant contracts with these third parties are reviewed and approved by the Wellesley College Purchasing Department to ensure that the contracts contain the necessary language regarding safeguarding Personal Information. It is the responsibility of the primary budget holders to confirm that the third parties are required to maintain appropriate security measures to protect Personal Information consistent with this Program and Massachusetts laws and regulations.

Computer system safeguards

The ISO monitors and assesses 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 Personal Information, the College has implemented the following:

- 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 regularly.
    - Server accounts are locked after 3 successive failed password attempts.
    - Computer access passwords are disabled prior to an employee's termination.
    - User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.
- Secure access control measures
    - Access to specific files or databases containing Personal Information is limited to those employees who require such access in the normal course of their duties.
    - Each such employee has been assigned a unique password, different from the employee's password to the computer network, to obtain access to any file or database that contains Personal Information needed by the employee in the course of his or her duties.
- Files containing Personal Information transmitted outside of the Wellesley College network are encrypted.
- The ISO performs regular internal network security audits 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 Personal Information.

- 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, and the entire system is tested and checked at least once per month.

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 Personal Information. The ISO maintains appropriate records of all such training.

Policies cross-referenced

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

- Records Management Policy
- FERPA policy
- Red Flag Policy
- Business Conduct Policy
- Employee Confidentiality Policy
- Responsible Use of Information Technology Resources

Effective date

This Written Information Security Program is effective February 1, 2010.

The College will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.