# Wellesley College Data Incident Response Plan

## 1.0 Policy Statement

The *Wellesley College Data Incident Response Plan* outlines the College's actions following a data breach or other type of data related incident in order to ensure timeliness of response, compliance with applicable laws and regulations and ensure consistency in all aspects of the College's response.

## 2.0 Background

The number of data breaches worldwide increases every year, as a result of hackers attempting to capture confidential and/or protected information. Academic institutions are at risk because of the kinds of sensitive information they maintain. Data breaches can occur anywhere that information resides, including computer systems, portable media, paper records, etc.

Wellesley College is committed to protecting the privacy of its community, which includes safeguarding the sensitive and protected data that is owned and maintained by the college. Wellesley College has taken many steps to reduce the risk of breach of such data, many of which are outlined in the College's Written Information Security Program (WISP). However, no protection is foolproof, and many data breaches occur as a result of human error. Therefore, Wellesley College must be prepared to respond to a breach in the event that one should occur.

## 3.0 Purpose

In accordance with federal and state laws and regulations, Wellesley College is required to provide notice about security breaches of protected information at the college to affected individuals and appropriate state agencies. Wellesley College is also committed to protect other kinds of sensitive institutional information that is maintained at the College. In the event that sensitive and/or protected information at Wellesley College is exposed as a result of a breach, the College must take steps to:

- Prevent further exposure,
- Investigate the incident and support law enforcement if criminal activity is suspected,
- Determine any legal obligations,
- Notify the departments and individuals affected,
- Respond to media inquiries,
- Document any responsive actions taken, and
- Conduct a post-incident review of these actions.

Accomplishing the above tasks will necessarily involve individuals from diverse areas of the College and will require that a plan be in place to address a breach before it occurs. The purpose of this plan is to outline the College's response to a data breach, including procedures for reporting a breach and individual team members' responsibilities following a breach.

## 4.0 Scope

The Incident Response Plan addresses four types of information compromises:

1. Computing Devices Compromised by Malware
2. Computing Devices Compromised by Unauthorized Access (includes any devices accessed without permission, either by stolen or compromised credentials, or other attempts to access a device without authorization)
3. Lost or Stolen Computing Devices
4. Lost or Stolen Paper Records containing Confidential Data, as defined below

The scope includes all computing devices (both College-owned and personal), including computers, servers, portable media, external hard drives or other mobile devices, and all paper records, which contain Confidential data. **All Wellesley College employees that maintain or access Confidential data, both paper and electronic, at the college must comply with this plan.**

## 4.1 Definitions

**Breach of security:** The unauthorized acquisition or use of sensitive or protected data that creates a substantial risk of identity theft, fraud or harm to the reputation or business interests of an individual or institution.

**Compromised computer:** Some ways a compromised computer can be identified include: the computer user suspects that his/her system is exhibiting suspicious behavior or has suspicious files stored on the device; network or system logs indicate unusual network behavior coming from or going to the device; or individuals at Wellesley College or outside of the College report cyber-attacks or unusual network behavior emanating from the device.

**Confidential data:** Refers to any information, both paper and electronic, that is protected by Federal, state, or local laws and regulations, or other sensitive personal and institutional data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operations or reputation of Wellesley College. Protected data includes Personal Information (defined below), student education records, and Protected Health Information (PHI). For a more complete description of these terms and the types of data identified as Confidential, see the College's Written Information Security Program (WISP) and the related policies cross-referenced at the end of this document.

**Personal Information:** Personal Information (PI), as defined by Massachusetts law (201CMR17.00), is 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: 1) Social Security number; 2)Driver's

license number or state-issued identification card number; or 3) Financial account number (e.g. bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password. As defined by the WISP, PI also includes passport number, alien registration number or other government-issued identification number.

**Wellesley College employees:** Includes all Wellesley College employees, whether full- or part-time, including faculty, administrative staff, union staff, contract and temporary workers, hired consultants, interns, and student employees.

## 5.0 Responsibilities

The College's Information Security Officer (ISO) is charged with the identification of all data security incidents involving electronic data or paper records where the loss, theft, unauthorized access, or other exposure of Confidential data is suspected. When the ISO confirms an incident involving Confidential electronic data, the ISO will alert the Chief Information Officer (CIO). The CIO will contact the Chair of the Incident Team - the Assistant Vice President for Finance - who will convene the Data Incident Team. In the event the Assistant Vice President for Finance is unavailable, the Risk and Compliance Manager will assume the role of Chair in his or her absence. The Chair of the Team is responsible for coordinating the Data Incident Team and determining appropriate actions in their response to the breach.

The Data Incident Team includes representatives from a number of college departments including the Assistant VP for Finance (or his or her designee), Assistant VP for Communication & Public Affairs, Director of Internal Communications, Risk and Compliance Manager, Chief of Campus Police, the CIO (or his or her designee) and the ISO. The Chair, in consultation with the Data Incident Team, will determine which additional members of the campus community will respond to the breach depending on the nature of the incident and the type(s) of information involved.

The Chair will oversee the investigation of the incident and involve legal counsel, local, state, and federal law enforcement as necessary. The severity of the breach will determine the nature of the investigation, including what authorities are involved and how evidence is collected.

The ISO will document all breaches and subsequent responsive actions taken. All related documentation will be stored in the Finance Office.

All Wellesley College employees are responsible for identifying and reporting potential security breaches. For help with security issues, including descriptions of the various types of security breaches and how to report them, see the LTS security website.

## 6.0 Response Plan

For suspected data breaches, the ISO will:

1. **Conduct a preliminary investigation:** Gather details about the incident, including when the breach was first discovered and how the employee responded. In cases involving electronic data, the ISO will also inquire about symptoms of the compromised computing device.
2. **Determine if Confidential data was involved**: Inquire about the nature of records or data involved in the breach and what kinds of information it contained. For electronic data breaches, the ISO will use a variety of technologies to determine if Confidential data was present on the compromised device. If the computing device was stolen, the ISO will do the analysis on backups. If backups are not available, the severity of the incident will be classified based on the individual's access to various sensitive data.

If an incident involving Confidential data is confirmed, the ISO will contact the Chair of the Incident Team. The Chair will:

1. **Notify Senior Staff:** Provide details about the incident and provide status updates.
2. **Convene the Incident Team:** If PI, PHI or student education records were determined to be involved in the data breach, or if the presence of sensitive data could not be ruled out, the Chair will convene the Incident Team.
3. **Consult Legal Counsel:** The Chair and Incident Response Team will consult the College's legal counsel to review the incident to determine the College's legal obligations for reporting under applicable federal and state laws.
4. **Notify affected individuals:** Under Massachusetts General Law Chapter 93H, and The Health Information Technology for Economic and Clinical Health (HITECH) Act, the College is required to notify any individuals whose personal information or protected health information (respectively) may have been compromised as a result of this incident (regardless of confirmation of identity theft). Depending on the circumstances of the breach, the College may be obligated to notify other individuals and agencies as prescribed as law. The nature of the breach will also determine the method(s) of notification.

## 7.0 Enforcement

Any employee who neglects to report a known security breach, or who fails to comply with this plan in any other respect, will be subject to disciplinary action.

## 8.0 Policies Cross-Referenced

FERPA Policy
HIPAA Privacy Notice
Written Information Security Program

## 9.0 Effective Date

This plan is effective May 3, 2013.