Written Information Security Program

Policy Statement

The Bay Path University Written Information Security Program (WISP) is intended to establish a set of guidelines and policies to ensure the safety of all sensitive data stored within the systems owned and operated by the University, and to comply with applicable laws and regulations in regards to the protection of personal information stored within the University's records and information systems. This WISP will be reviewed and amended as necessary to protect personal information. The University has implemented a number of policies to protect such information, and the WISP should be read in conjunction with the policies that are cross-referenced at the end of this document.

Purpose

The WISP has been implemented to comply 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].

In accordance with federal and state laws and regulations, Bay Path University has taken steps to safeguard personally identifiable information, and to provide notice about security breaches of personal information at the University to impacted individuals and inform appropriate state agencies.

The University has implemented a number of policies to protect sensitive information, and the WISP should be read in conjunction with the policies that are cross-referenced at the end of this document.

Scope

The WISP applies to all Bay Path University faculty, staff and students, as well as to all other members of the Bay Path University community (hereafter referred to as the "community"). The data covered by the WISP includes any information stored, accessed or collected by the University or for University operations. The WISP is not intended to supersede any existing University policy that contains more specific requirements for safeguarding certain types of data, except in the case of personal Information. If such policy exists and is in conflict with the requirements of the WISP, the other policy takes precedence.

Definitions

Personal Information

Personal Information (PI), as defined by Massachusetts law (201 CMR 17.00), 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:

- Social Security number
- Driver’s license number or state-issued identification card number
- 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.

Data

For the purposes of this document, data refers to information stored, accessed or collected at the University about members of the community.

Data Custodian

A data custodian is responsible for maintaining the technology infrastructure that supports access to the data, safe custody, transport and storage of the data and provide technical support for its use. A data custodian is also responsible for implementation of the business rules established by the data steward.

Data Steward

A data steward is responsible for the data content and development of associated business rules, including authorizing access to the data.

Data Classification

All data covered by this policy will be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level.

Confidential

Confidential data refers to any data where unauthorized access, use, alteration or disclosure of this data could present a significant level of risk to the University or the community. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration or disclosure.

Confidential data includes data that is protected by the following federal or state laws or regulations: 201 CMR 17.00 (Mass Security Regs), and Health Insurance Portability and Accountability Act of 1996 (HIPAA). Information protected by these laws includes, but is not limited to, PI, and Protected Health Information (PHI).

Restricted

Restricted data refers to all other 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 Bay Path University. Any non-public data that is not explicitly designated as confidential should be treated as restricted data.

Restricted data includes data protected by the Family Educational Rights and Privacy Act (FERPA), referred to as student education records. This data also includes, but is not limited to, donor information, research data on human subjects, intellectual property (proprietary research, patents, etc.), University financial and investment records, employee salary information, or information related to legal or disciplinary matters.

Restricted data should be limited to access by individuals who are employed by or matriculate at the University and who have legitimate reasons for accessing such data, as governed by FERPA, or other applicable law or University policy. A reasonable level of security should be applied to this classification to ensure the privacy and integrity of this data.

Public

Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to the University or members of the community. Any data that is not classified as Confidential or Restricted should be considered public data.

Policy

Information Security

Policies and procedures created by Information Security will be reviewed by senior staff and University Leadership prior to implementation.

Information Security, along with the IT Director and IT Staff, are responsible for:

- Performing an annual review of the WISP to account for any newly identifi ed risks to paper or electronic records containing qualifying personal information as defined by MA 201 CMR 17.00.
- Evaluating the ability of all 3rd party vendors and service providers working under contract with Bay Path University to comply with MA 201 CMR 17.00. Bay Path University will require all providers, when applicable, to include a written statement verifying that they are in full compliance with MA 201 CMR 17.00. Bay Path University will notify all vendors of the University's intent to review all existing contracts to determine which vendors will be required to submit written verification of their compliance with MA 201 CMR 17.00.
- Assist departments employing work-study students with potential access to person al information records in developing a training program for this population. All work-study students will be required to review and sign the University policy regarding confidentiality and proprietary information prior to working on campus. All work-study supervisors will be required to review and collect the Work-Study Responsibilities and Procedures form from their student workers prior to the student working for their department.

Responsibilities

All data at the University is assigned a data owner according to the constituency it represents. Data owners are responsible for approval of all requests for access to such data. The data owners for each constituency group are designated as follows:

- **Faculty data** - The Provost (or designee) serves as the data owner
- **Staff data** - The Vice President for Finance & Administrative Services (or designee) serves as data owner
- **Donor data -** The Vice President of Development (or designee) serves as the data owner
- **Student data** - Ownership is distributed across many departments. A Bay Path University policy regarding student data ownership is currently being developed. The ITS Director will act as data steward for student data in the interim.

Information Technology Services (ITS) staff serve as the data steward for all data stored centrally on the University's servers and information systems, and are responsible for the security of such data. For distributed data stored on servers not under the purview of ITS, the department head or their designee serves as the data steward, and ITS and the department share joint responsibility for securing the data.

Human Resources will inform ITS staff about an employee's change of status or termination as soon as is practicable but before an employee's departure date from the University. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to University data. ITS staff will terminate all of the employee's account access upon the employee's termination date from the University, as specified by Human Resources.

Department heads will alert ITS at the conclusion of a contract for individuals that are not considered University employees in order to terminate access to their University accounts. University Information Security, along with the ITS DIrector, is in charge of maintaining, updating, and implementing this Program. All members of the community are responsible for maintaining the privacy and integrity of all sensitive data as defined above, and must protect the data from unauthorized use, access, disclosure or alteration. All members of the community are required to access, store and maintain records containing sensitive data in compliance with this Program.

Identification and Assessment of Risks to University Information

Bay Path University recognizes that it has both internal and external risks to the privacy and integrity of University information. These risks include, but are not limited to:

- Unauthorized access of confidential or restricted data
- Compromised system security as a result of system access by unauthorized person(s)
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized transfer of confidential or restricted data through third parties

Bay Path University recognizes that this may not be a complete list of the risks associated with the protection of sensitive data. Since technology is ever changing, new risks are created regularly. Accordingly, ITS will actively participate and monitor advisory groups such as the Educause Security Institute, REN-ISAC and SANS for identification of new risks. Bay Path University believes the University's current safeguards are reasonable and are sufficient to provide security and confidentiality to sensitive data maintained by the University. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

Safeguarding Sensitive Data

To protect sensitive data, 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 sensitive data in the regular course of their duties are granted access to sensitive data, including both physical and electronic records.
- Computer and network access accounts are disabled upon termination of employment or relationship with Bay Path University.
- Upon termination of employment or relationship with Bay Path University, physical access to documents or other resources containing sensitive data is immediately prevented.
- Elevated system privileges must be approved by the ITS director or their designee. Employees with elevated system privileges may only use those privileges when necessary to perform specific system related tasks that are directly related to their job. Those privileges should never be used to access data of any type that the employee does not normally have access to.

Storage

- Members of the community will not store sensitive data on laptops or on other mobile devices (e.g., flash drives, smart phones, external hard drives) unless those devices are encrypted with the current standard encryption process as established by the ITS Department.
- To the extent possible, making sure that all sensitive data is stored only on secure servers maintained by the University and not on local machines, insecure servers, or portable devices.
- Paper records containing sensitive data must be kept in locked files or other secured areas when not in use.
- Electronic records containing sensitive data must be stored on secure servers, and, when stored on authorized desktop computers, must be password protected.
- Massachusetts PI must not be stored on Google Docs or other types of "Cloud" services.

Removing Records from Campus

- Members of the community are strongly discouraged from removing records containing sensitive data off campus. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing sensitive data to be left unattended in any insecure location.

- When there is a legitimate need to provide records containing sensitive data to a third party, electronic records shall be password-protected and/or encrypted, and paper records shall be marked with the appropriate classification and securely sealed.

Destruction of Confidential Data

- Paper and electronic records containing confidential data must be destroyed in a manner that prevents recovery of the data. Massachusetts General Law 93I specifies the manner in which records containing PI must be destroyed.

Third-Party Vendor Agreements Concerning Protection of Personal Information

Bay Path University exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for PI provided by the University to them. The primary budget holder for each department is responsible for identifying those third parties providing services to the University that have access to PI. All relevant contracts with these third parties are reviewed and approved by the University's purchasing department to ensure the contracts contain the necessary language regarding safeguarding PI. It is the responsibility of the primary budget holders to confirm that the third parties are required to maintain appropriate security measures to protect PI consistent with the WISP and Massachusetts laws and regulations.

Computer System Safeguards

The Information Security Manager monitors and assesses information safeguards on an ongoing basis to determine when enhancements are required. The University has implemented the following to combat external risk and secure the University network and data containing PI:

- Secure user authentication protocols
- Unique passwords are required for all user accounts; each employee receives an individual user account.
- Service accounts are locked after multiple unsuccessful password attempts.
- Computer access accounts are disabled upon an employee’s termination.
- User passwords are stored in an encrypted format; root passwords are only accessible by system administrators and are stored in an encrypted format.
- Secure access control measures.
- Access to specific files or databases containing PI 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 PI needed by the employee in the course of his or her duties.
- Files containing PI transmitted outside of the University network are to be encrypted.
- Information Security 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 PI.
- All University-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

Employee Training

All employees who access Confidential data via the firewall or who otherwise have access to PI are required to complete a yearly training on data security and their responsibilities related to this Program. The training is also strongly recommended for all employees.

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 PI, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the ISD.

The ITS Director is charged with the identification of all data security incidents where the loss, theft, unauthorized access, or other exposure of sensitive University data is suspected. Any such incidents should be reported to University Executive Staff. Executive Staff is responsible for determining appropriate actions in their response to the breach under the advisement of the ITS and Information Security.

All breaches and subsequent responsive actions taken will be documented by Information Security and ITS. All related documentation will be stored in the Finance Office.

Enforcement

Any employee or student who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises data classified as confidential or restricted 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 cross-referenced

The following Bay Path University policies provide advice and guidance that relates to this program:

- Acceptable Use Policy
- Operations Manual
- FERPA Policy
- HIPAA Privacy Policy
- Password Guidelines

Effective date

This Written Information Security Program was implemented January 1, 2014 and last updated on December 12, 2017. The University 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.