Written Information Security Plan

1.0 Overview

WPI's objective in the development and implementation of this Written Information Security Plan is to ensure effective procedural, administrative, technological and physical safeguards for protecting the personal information of Faculty, Staff, Students, Alumni, customers and residents of the Commonwealth of Massachusetts, and to ensure compliance with Massachusetts Law 201 CMR 17.00.

This WISP sets forth WPI's procedures for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII (Personally Identifiable Information- see definitions below).

2.0 Reason for the Plan

In formulating and implementing the WISP, WPI seeks to:

1. Identify reasonably foreseeable internal and external risks to the security and confidentiality of any electronic, paper, or other records containing PII;
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
3. Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. Identify existing policies and procedures that serve as resources for WPI to further enhance and comply with security issues;
5. Design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00;
6. Regularly monitor the effectiveness of those safeguards.

WPI has made the affirmative decision to identify what is and is not PII, and has declined the invitation to treat all records it maintains as PII.

3.0 Definitions

1. WISP

The term "WISP" refers to WPI's Written Information Security Plan.

2. PII

The term "PII" shall mean "Personally Identifiable Information." PII is encompassing of any and all data regarding Massachusetts residents held by WPI, written or electronic, the improper disclosure of which would trigger written notification to both the Massachusetts Attorney General and the affected Massachusetts residents.

WPI follows the statutory definition of "personal information" as it is used in 201 CMR 17.00. As such, PII means a Massachusetts resident's first name and last name, or first initial and last name in combination with any one or more of the following data elements which relate to such resident (a) Social Security Number, or truncated Social Security Number (b) Driver's License number or state-issued identification card number, or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number ("PIN") or password that would permit access to a resident's financial account. PII does not include that information which is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

3. Breach

A "breach" shall mean the unauthorized acquisition or unauthorized use of either unencrypted PII or, encrypted electronic PII along with the confidential decryption process or key that is capable of compromising the security, confidentiality, or integrity of PII maintained by the University, creating a substantial risk of identity theft or fraud against a resident of the Commonwealth.

A good faith but unauthorized acquisition of PII by a person, for the lawful purposes of such person, is not a breach unless the PII is used in an unauthorized manner or subject to further unauthorized disclosure.

A "breach" shall not include disclosure of PII which is legally accessible from an outside legitimate source, or where disclosure is required by court order or where necessary to comply with state or federal regulations.

4. Data Security Manager

The University has identified WPI's Chief Information Security Officer (CISO) as the Data Security Manager. The CISO has the following responsibilities:

- Implementation of the Plan;
- Regular testing of the Plan's safeguards;
- Evaluating the ability of service providers to comply with 201 CMR 17.00 in the handling of personal information for which we are responsible, ensuring there are included in our contracts with those services providers provisions obligating them to comply with 201 CMR 17.00 in providing the contracted for services, and obtaining from such service providers written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of 201 CMR 17.00.
- Reviewing the scope of the security measures in the Plan at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information.

5. Data Security Coordinators

The Data Access Working Group and the Data Stewards are designated as the Data Security Coordinators and are responsible for:

- Protecting personal information collected as written or digital data University wide by ensuring all employees handling personal identification data are properly trained:
- Educating all data owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the Plan.
- Ensuring campus wide compliance with this policy and the WPI Security Policies.

4.0 Statement of Policy

1. Commitment to Limited Collection of, and Access to, PII

WPI will collect, maintain and store only that PII which is reasonably necessary to accomplish the legitimate business purpose for which it is collected; limiting the time PII is retained to what is reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to have access to PII in order to accomplish such purpose or to comply with state or federal record retention requirements. All persons granted access to PII shall be informed of WPI's Written

Information Security Plan and shall be provided basic training for compliance with its requirements.

2. Identified Locations of PII

WPI has identified specific electronic databases and servers, along with physical locations, where PII is known to exist. These locations, while not an exhaustive list, are kept by the Chief Information Security Officer (CISO) and Data Security Coordinators and are audited by the CISO. It is incumbent upon the Data Security Coordinators in each department, to promulgate amongst their staff with PII access, any and all identified locations of PII they have access to, and the importance of preserving its confidential nature.

3. Identification and Assessment of Risks to University Information

WPI 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 data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- 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 access of Confidential data by employees
- Unauthorized requests for Confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential data through third parties

WPI recognizes that this may not be a complete list of the risks associated with the protection of confidential data. WPI believes the University's current safeguards are reasonable and are sufficient to provide security and confidentiality to confidential data maintained by the University.

Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

4. Electronic Data Safeguards

- **Identity Management:** WPI will maintain a procedure for managing computer accounts for active employees, and will have in place procedures for promptly disabling accounts of those individuals who are no longer employed and/or entrusted by the University.
- **Passwords:** WPI requires passwords for accessing any system that may contain PII. Passwords must meet minimum requirement of complexity set by the CISO. Accounts shall be locked after excessive unsuccessful login attempts. Enforcement of the password policy shall be maintained through electronic means. Vendor assigned and default passwords shall be changed reasonably promptly, but must be changed before the system accessed through said password contains any PII. Access to PII shall be electronically limited to those employees with unique usernames. Usernames and passwords with access to PII shall not be shared amongst individuals.
- **Network Design Considerations:** WPI shall maintain its firewall and intrusion prevention systems so that networks with data servers can be isolated from end-user systems.
    - **Firewall:** A commercial-grade firewall shall be maintained at WPI protecting systems containing PII from both external and internal unauthorized access. The software running on the firewall shall be reasonably current.
    - **IPS:** WPI has as part of its firewall an Intrusion Prevention System that monitors traffic across its network to help mitigate against unauthorized access. The software shall be kept reasonably current.
- **Data Encryption:** Where electronic files containing PII must unavoidably be taken from an approved storage location and placed on portable media (including, but not limited to, a computer's internal hard drives, USB "thumb drives," externally connected drives and other removable media), the files containing PII must comply with the standards set in the WPI Data Classification and Usage Policy.
- **Encrypted Network Transmission:** Where feasible, when PII is transmitted over a data network where data interception is reasonably foreseeable, PII will be encrypted using WPI approved encryption. WPI shall maintain SSL Certificates, managed by a trusted root host, which shall be used on web pages served by the University over which there exists the reasonably foreseeable possibility that PII may be accessed.
- **VPN**: WPI shall maintain a Virtual Private Network ("VPN"), which will necessarily be used to encrypt data connections to the University where there is a reasonably foreseeable possibility that PII will be carried over the connection and an SSL HTTP connection is not feasible.
- **System Hardening and Security Patches**: WPI's Systems will be security hardened with current security configurations and removal any default credentials. Reasonable

means and methods shall be taken to ensure that security-related critical patches are applied to operating systems and application software.

- Anti-Virus and Malware: There shall be reasonably up-to-date versions of virus/malware protective agents running on University-owned computers, which report to a central server that is reviewed regularly for compliance with policy.
- Electronic File Storage: The University shall maintain a file server or other secure means of data storage of sufficient speed and storage capacity to hold any and all electronic documents that may contain PII. No PII should be stored on individual desktop/laptop computers. All data must comply with WPI's Data Classification and Usage Policy.
- Encrypted Backups: Wherever feasible, server backups shall be encrypted using an industry-accepted data encryption standard.
- Ongoing Data Security Training and Acceptable Use: The University shall maintain an information security employee training program. Employees whose positions at the University require contact with PII shall be provided additional training, within their departments, commensurate with the potential exposure. The University will maintain an acceptable use policy with which all persons granted access to WPI's network will be required to comply.

5. Data Retention and Destruction

- Destruction of records will be done in a commercially acceptable manner so that PII cannot be practically read or reconstructed, via either a University approved shredding service or a cross-cut shredder.
- All hard drives from servers or sensitive computer systems designated for replacement or retirement must be erased using DOD approved software or securely destroyed to render any PII data unreadable or unable to be reconstructed.
- Where the University contracts with a third-party data destruction company, the University shall obtain written assurances from the third-party that its disposal practices are in compliance with M.G.L. Ch. 93I
- All data retention must comply with the Records Retention and Destruction Policy.

6. Paper Based Data Safeguards

- File Cabinets: Where filing cabinets are to be used for the storage of PII, the filing cabinets are to remain locked unless the need to access the files within is imminent or current. Should removal of files containing PII from a filing cabinet be necessary, the files themselves must be protected against unauthorized access and if the files will not be returned to the filing cabinet promptly, the filing cabinet shall be locked. Files must be returned to filing cabinets, which are then to be locked, no later than the end of the workday of the employee that removed them, unless their

overnight storage outside their designated filing cabinet is approved, in writing, by the appropriate Data Security Coordinator.

- Transport: All efforts will be made to minimize the physical transport of printed PII, substituting encrypted electronic data transport instead. Where printed PII must be transported, the carrier shall either be commercial and bonded, or a trained member of the WPI community.

7. Third Party Entrustment

- WPI shall take all reasonable steps to verify that any third-party vendor, contractor or service provider with access to PII maintained by the University has the capacity to protect such PII in the manner required by 201 CMR 17.00.
- WPI requires that all third-party vendors, contractors or service providers entrusted with PII complete, and submit to the University, a written manifestation of their current and ongoing compliance with the requirements of 201 CMR 17.00. Should the third-party not provide such documentation, or later withdraw their assent to the requirements, the University shall no longer provide any PII to said third-party and will take affirmative steps to ensure that previously entrusted PII is destroyed in a manner in-line with that which the University would use.
- All vendor contracts that will have access to PII must include standard WPI contract language for PII.

8. Termination of the Relationship that Requires Entrustment of PII

Employees may leave, be terminated, or switch roles within WPI. The relationship between WPI and third parties may change. Where the employee or third party had access to specific PII and the changed relationship negates the need for access, WPI shall take specific affirmative steps to ensure that access to PII is withdrawn.

- All records containing PII, in any form, must be returned at the time of termination of the relationship. If return is not feasible, destruction in accordance with industry standards, along with proof of such destruction, is acceptable.
- At the time of termination of the relationship, all electronic and physical access to PII must immediately cease and be blocked. Former employees and third parties must return keys, IDs (if not required for other legitimate purposes), access control tokens and cards. Electronic locks access shall be disabled.
- Continued access to PII by former employees and third parties with whom the business relationship has been terminated must be expressly authorized, in writing, by the appropriate Data Security Manager.

9. Breach Procedures

Whenever there is a breach that requires notification under M.G.L. Ch. 93H § 3, the University shall take, at a minimum, the following steps:

- A letter shall be sent to the Massachusetts State Attorney General and the Director of Consumer Affairs and Business Regulations.
- A letter shall be sent by the Office of General Counsel and Chief of Staff to the affected Massachusetts residents notifying them of the breach.
- A letter of notification of breach shall be sent to the University's insurance carrier.
- An immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in the security practices are required to improve the security of PII.
- Disciplinary action may be taken against the individual, or individuals, who caused, or contributed to, the breach.

5.0 Enforcement

Any person that violates any of the measures found in this plan will be subject to the same disciplinary actions outlined in WPI's Confidentiality Agreement for employees, or the Acceptable Usage Policy and Code of Conduct for students.

6.0 Cross References to Related Policies

Confidentiality Policy
Data Classification and Usage Policy
Records Retention and Destruction Policy
Data Breach Procedure

7.0 Approval and Revisions

Policy Category: Institutional Risk & Compliance
Policy Approved By: Approved by WPI's Information Security, Risk and Compliance Committee on 09/26/2018.
Policy Reviewed Annually By: Sean O'Connor
Last Modified: 9/20/18