FISHER COLLEGE

Comprehensive Written Information Security Program

In compliance with the Commonwealth of Massachusetts, 201 CMR 17.00

European Union General Data Privacy Regulations Policy, attached as Addendum II

I. Purpose

The development and implementation of the Fisher College Written Information Security Program ("WISP") is to create effective administrative, technical, and physical safeguards for the protection of Personal Information, and to comply with the obligations of the Commonwealth of Massachusetts under the regulations found at 201 C.M.R. 17.00 *et seq*. Personal Information, as defined for this Program, 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 that relate to such resident: (a) 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 or password that would permit access to a resident's financial account. Personal Information, however, does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully available to the general public.

Though expressly intended to address its obligations to the Commonwealth, the provisions of this policy are intended to extend to encompass all individuals and all related personal information associated with the College. In addition, the policy is intended to function in unison with the Fisher College Identity Theft Prevention Program, as approved by the College on October 1, 2009, and written in compliance with the Red Flag Rule of the Federal Trade Commission, implementing Section 114 of the Fair and Accurate Credit Transactions Act.

II. Scope

It is the intention of the WISP to establish safeguards to protect Personal Information that is owned, licensed, stored or maintained by the College, whether this information is filed on paper, electronically, or on any other format. The WISP is intended to ensure the overall integrity and confidentiality of Personal Information in all existing formats, to guard against threats to its security, and to protect against unauthorized or prohibited access to Personal Information from any conduct which could generate risk of fraud or identity theft.

III. Administration

The Fisher College Data Privacy and Compliance Committee is designated as the Program Administrator of the WISP. The Committee will appoint one of its members to be named "Information Security Coordinator" for this Program. The Committee and the Information Security Coordinator will be responsible for:

A. Initial implementation of the WISP;
B. Employee training;
C. Regular testing of the WISP's safeguards;
D. Evaluating the ability of third party providers to implement and maintain appropriate security measures for Personal Information to which the College has permitted them access;
E. Reviewing the scope and effectiveness of the WISP annually, at minimum, or when there are deemed to be material changes to policies, practices or technology which may jeopardize the integrity of the WISP or the security of Personal Information. Based on such reviews, the Program will be updated accordingly.

IV. Personal Information

Practices for the creation, access, transmission, and disposition of all documentation containing Personal Information are to be managed according to the following methods:

A. All files containing Personal Information must be identified as confidential upon their creation. Documents or files identified as confidential and containing Personal Information cannot be left unattended or unsecured at any time. Paper documents must be stored in a locked desk, file cabinet, office, or controlled area, and any unattended areas containing Personal Information files must be locked and secure at all times. Physical access to records and files by unauthorized personnel is strictly prohibited. Storage of electronic Personal Information must be kept to a minimum, and encrypted when feasible.
B. Access and disclosure of Personal Information must be limited to individuals who are reasonably required to utilize this information for justifiable school or business purposes. Information may also be released when required by state, local, or federal regulation or requirement. Prior to engaging third-party service providers, the College will conduct reasonable due diligence to assess whether the provider is capable of safeguarding Personal Information in a manner required by the Fisher College WISP. These providers should be periodically monitored to assure their

Personal Information protective measures remain compliant with the requirements of this Program.

C. Physical transmission between locations of paper or hard-copy format documentation containing Personal Information must be done with reasonable precaution. Voice communication of Personal Information should always be performed in a secure location.
D. Personal Information should be disposed of following the retention period dictated by federal, state, or local requirements, and following a time reasonably necessary to accomplish a legitimate business purpose. Paper or hard-copy documents should be disposed of by cross-cut shredding, incineration, pulping, or burning. Electronically stored Personal Information should be destroyed or erased to the extent that Personal Information cannot practically be reconstructed.

V. Information Technology Policies and Procedures

Policies and procedures of the Fisher College Information Services Department shall contain the following safeguards:

A. Firewall protection must be reasonably up-to-date, and operating system security patches reasonably designed to maintain the integrity of Personal Information must be installed on all systems processing Personal Information.
B. There must be reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing Personal Information.
C. All Personal Information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible.
D. All computer systems must be monitored for unauthorized use or access.
E. There must be secure user authentication protocols in place, including: (a) protocols for control of user IDs and other identifiers; (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies such as biometrics or token devices; (c) control of data security passwords to ensure that such passwords are kept in a secure location; (d) electronic access via secure user identifiers to systems containing Personal Information must be blocked after multiple unsuccessful attempts have been made to gain entry.

VI. Awareness, Compliance and Risk Assessment

The Information Security Coordinator shall coordinate training regarding the Fisher College WISP. Training shall be mandatory for all employees having access to Personal information. The Information Security Coordinator shall also ensure that this Program shall be communicated to all consultants, volunteers, and third party service providers having access to Personal Information.

All employees (whether full-time, part-time, substitute, seasonal, or temporary), and all independent contractors, consultants and volunteers are subject to the applicable requirements set forth in this Program.

In the event suspicious activity involving Personal Information is suspected, or an individual has reason to believe that the Personal Information of any individual has been violated, such activity must be reported to their supervisor immediately. Subsequently, the supervisor should report the incident to the Information Security Coordinator or any member of the Data Privacy and Compliance Committee. If warranted, the Committee will follow procedures as set forth by the Commonwealth under Chapter 93H (Addendum I.) A post-incident review of the events and of subsequent actions taken will be conducted by the Privacy, Security and Identity Theft Committee.

Instances of non-compliance with this Program must be reported immediately to the Information Security Coordinator. Violations may result in disciplinary action, including termination of employment. It is unlawful to retaliate against any individual who reports a violation of non-compliance of this Program.

Terminated employees, or employees, consultants and volunteers who have separated from service to the College for any reason, are required to surrender all keys, IDs, access codes, badges, business cards, and the like, that permit access to property or premises containing Personal Information.

The Data Privacy and Compliance Committee shall, on a periodic basis, conduct a risk assessment to evaluate internal and external effectiveness of compliance with the Fisher College Written Information Security Program, including but not limited to the evaluation of ongoing employee training, changes and advances in technology, changes in identity theft methods, and any other factors deemed relevant to maintaining the security and integrity of Personal Information.

Fisher College WISP

Addendum I.

Requirements for Security Breach Notifications under Chapter 93H

Where a person who owns, licenses, maintains or stores personal information, knows or has reason to know (1) of a security breach, or (2) that the personal information of a Massachusetts resident was acquired or used by an unauthorized person or for an unauthorized purpose, that person must notify the Attorney General and the Office of Consumer Affairs and Business Regulation of that breach or unauthorized acquisition or use.

A "security breach" is defined in the law as "the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure."

"Personal information" is defined in the law as "a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) 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 or password, that would permit access to a resident's financial account." Excluded from "personal information" is information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."

The notifications to the Office of Consumer Affairs and Business Regulation and to the Attorney General must include:

- A detailed description of the nature and circumstances of the breach of security or unauthorized acquisition or use of personal information;
- The number of Massachusetts residents affected as of the time of notification;
- The steps already taken relative to the incident;
- Any steps intended to be taken relative to the incident subsequent to notification; and
- Information regarding whether law enforcement is engaged investigating the incident.

Addendum II – European Union General Data Privacy Policy

I. OBJECTIVE

The aim of this EU Privacy Policy ("the Policy") is to provide adequate and consistent safeguards for the handling of Personal Data (as defined below) by Fisher College ("Fisher" or the "College") in accordance with the General Data Protection Regulation.

II. SCOPE

This Policy applies to all Fisher College departments that process Personal Data.

"Consumer" means any natural person who is located in the EU, but excludes any individual acting in his or her capacity as an Employee. Consumers include, but are not limited to students, applicants, vendors and other third party providers of services.

"Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data as referred to in Privacy Shield materials.

"Employee" means any current, former or prospective employee, temporary worker, intern or other non-permanent employee of Fisher College.

"European Economic Area ("EEA")" means the following countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Republic of Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the UK.

"Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity and includes information, that (i) relates to an identified or identifiable Employee or Consumer; (ii) can be linked to that Employee or Consumer; (iii) is transferred to Fisher College in the U.S. from the EEA or Switzerland, and (iv) is recorded in any form.

“Privacy Shield” means the EU-US Privacy Shield framework and agreement between the United States of America, via the US Department of Commerce and the EEA relating to the protection of Personal Data.

“Sensitive Personal Data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning health or sex, and the commission or alleged commission of any offense, any proceedings for any offense committed or alleged to have been committed by the individual or the disposal of such proceedings, or the sentence of any court in such proceedings.

“Processing” is defined as any action that is performed on Personal Data, whether in whole or in part by automated means, such as collecting, modifying, using, disclosing, or deleting such data.

This Policy does not cover data rendered anonymous or where pseudonyms are used. Data is rendered anonymous if individuals are no longer identifiable or are identifiable only with a disproportionately large expense in time, cost or labor. The use of pseudonyms involves the replacement of names or other identifiers with substitutes, so that identification of individual persons is either impossible or at least rendered considerably more difficult. If data rendered anonymous become no longer anonymous (i.e. individuals are again identifiable), or if pseudonyms are used and the pseudonyms allow identification of individual persons, then this Policy shall apply again.

III. APPLICATION OF LOCAL LAWS

This Policy is designed to provide compliance with all relevant applicable laws in the EEA and in particular those transposing the Directive. Fisher recognizes that certain laws might be modified to require stricter standards than those described in this Policy, in which case the stricter standards shall apply.

IV. PRINCIPLES FOR PROCESSING PERSONAL DATA

Fisher respects Employee, Consumer (including personnel of customers, suppliers, stakeholders, and third parties) privacy and is committed to protecting Personal Data in compliance with the applicable legislation in the EEA. This compliance is consistent with Fisher’s desire to keep its Employees and Consumers informed and to recognize and

respect their privacy rights. Fisher will observe the following principles when processing Personal Data:

Data will be processed fairly and in accordance with applicable law.
Data will be collected for specified, legitimate purposes and not processed further in ways incompatible with those purposes.
Data will be relevant to and not excessive for the purposes for which they are collected and used. For example data may be rendered anonymous if deemed reasonable, feasible and appropriate, depending on the nature of the data and the risks associated with the intended uses.
Data subjects will be asked to provide their clear and unequivocal consent for the collection, processing and transfer of their Personal Data.
Data will be accurate and, where necessary kept up up-to-date. Reasonable steps will be taken to rectify or delete Personal Data that is inaccurate or incomplete.
Data will be kept only as it is necessary for the purposes for which it was collected and processed. Those purposes shall be described in this Policy.
Data will be deleted or amended following a relevant request by the concerned data subject, should such notice comply with the applicable legislation each time.
Data will be processed in accordance with the individual's legal rights (as described in this Policy or as provided by law).
Appropriate technical, physical and organizational measures will be taken to prevent unauthorized access, unlawful processing and unauthorized or accidental loss, destruction or damage to data. In case of any such violation with respect to Personal Data, Fisher will take appropriate steps to end the violation and determine liabilities in accordance with applicable law and will cooperate with the competent authorities.

V. TYPES OF DATA PROCESSED

As permitted by local laws, Personal Data may include the following:

name;
contact information;
date of birth;
government-issued identification information, passport or visa information;
educational history;
employment and military history;
legal work eligibility status;
information about job performance and compensation;
financial account information;

other data collected automatically through the website (such as IP addresses, browser characteristics, device characteristics, operating system, language preferences, referring URLs, information on actions taken on our website, and dates and times of website visits).
Financial account information.

VI. WAYS OF OBTAINING PERSONAL DATA

Fisher College does not obtain any personal information about Employees or Consumers unless the Employee or Consumer has provided that information to Fisher College in a way providing for its clear and unequivocal consent to do so including but not limited to visiting Fisher's website, by completion of a written employment application, employee benefits application, insurance form, consent form, survey, or completion of an on-line or hard copy form. Employees and Consumers may choose to submit personal, private information by facsimile, regular mail, e-mail, or electronic transmission over our internal web site, interoffice mail, or personal delivery, as each of these methods may be deemed applicable each time.

VII. PURPOSES FOR PERSONAL DATA PROCESSING

Fisher College processes personal data for legitimate purposes related to human resources, student registration, business and safety /security.

VIII. SECURITY AND CONFIDENTIALITY

Fisher College is committed to taking appropriate technical, physical and organizational measures to protect Personal Data against unauthorized access, unlawful processing, accidental loss or damage and unauthorized destruction.

IX. RIGHTS OF DATA SUBJECTS

Any person has the right to be provided with information as to the nature of the Personal Data stored or processed about them by Fisher College and may request deletion or amendments.

All Employees and Consumers have access to their own personal information and may correct or amend it as needed. If access is denied, the Employee and Consumer has the right to be informed about the reasons for denial. The person affected may resort to the dispute resolution described in Section XIII as well as in any competent regulatory body or authority. Fisher College shall handle in a transparent and timely manner any type of internal dispute resolution procedure about Personal Data is conducted.

If any information is inaccurate or incomplete, the person may request that the data be amended. If the person demonstrates that the purpose for which the data is being processed in no longer legal or appropriate, the data will be deleted, unless the applicable law requires otherwise.

X. TRANSFERS

In connection with the activities described under Section VII, Fisher College may transmit Personal Data as needed to effect its business. Fisher will not disclose or share any personal information with any external entity or third party, except to an employee's designated insurance provider, employee benefits administrator, travel professionals, clients to illustrate experience and qualifications for business purposes or promotion and not beyond that, to third party vendors and/or marketers upon Consumer's explicit consent or as an employee or consumer may designate.

Other Third Parties: Fisher may be required to disclose certain Personal Data to other third parties: (i) As a matter of law (e.g. to tax and social security authorities); (ii) to protect Fisher's legal rights; (iii) in an emergency where the health or security of an employee is endangered (e.g. a fire); (iv) to Law Enforcement Authorities in accordance with the relevant legislation in the different EEA Member States including but not limited to legislation transposing the EU/2016/1148 concerning measures for a high common level of security of network and information systems across the Union ("the Network Information Security Directive").

Fisher complies with all the Privacy Shield Principles of the Privacy Shield and has taken the necessary actions to register within the Privacy Shield framework.

XI. ENFORCEMENT RIGHTS AND MECHANISMS

Fisher College will ensure that this Policy is observed and duly implemented. All persons who have access to Personal Data must comply with this Policy. Violations of the applicable data protection legislation in the EEA may lead to penalties and/or claims for damages.