1.0 Written Information Security Program - WISP

Objectives

The objectives in the development and implementation of this comprehensive written information security program (“WISP” or “Program”) are:

- To create effective administrative, technical and physical safeguards for the protection of Confidential Information maintained by the University, including sensitive personal information pertaining to the University’ s faculty, staff, students, parents of students, alumni, customers and residents of the Commonwealth of Massachusetts, as well as other confidential and sensitive institutional and third party information.
- To comply with our obligations under law including the financial customer information security provisions of the federal Gramm-Leach-Bliley Act (“GLB”), 15 USC 6801(b) and 6805(b)(2), and implementing regulations of the Federal Trade Commission codified at 16 CFR Part 314 and the Massachusetts personal information safeguards law M.G.L.c 93H, s. 2, and implementing regulations of the Massachusetts Office of Consumer Affairs and Business Regulation (“OCABR”) codified at 201 CMR 17.00 entitled “Standards for the Protection of Personal Information of Residents of the Commonwealth”.

Scope of the WISP & Key Program Design and Implementation Features

The WISP provides for, and was designed and developed, and will be implemented, to include the following key features, requirements and components:

- Identification of reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records, or other University Information, containing Confidential Information;
- Assessment of the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Confidential Information;
- Evaluation of the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks;
- Design and implementation of safeguards to minimize those risks; and
- Regular monitoring of the effectiveness of those safeguards.

Applicability

This Program applies to all University faculty and staff, whether full-time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the University, including any Third Party Provider providing services to the University ("University Users"), who create, use or otherwise access or interact with any University Information or University Information Resource.

This Program applies to all University Information, including all information collected, stored or used by or on behalf of any operational unit, department and person within the University community in connection with University operations. In the event that any particular information at Suffolk University is governed by more specific requirements under other University policies or procedures, the more specific requirements shall take precedence over this Program to the extent there is any conflict.

Definitions

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

Breach of Security
As defined by the Massachusetts Security Breach Law, M.G.L.c. 93H, s 1 and 3, a Breach of Security means the unauthorized acquisition or disclosure, or unauthorized use, of unencrypted data (or encrypted electronic data and the confidential process or key used to decrypt the encrypted data) that is capable of compromising the security, confidentiality or integrity of Massachusetts Personal Information. A good faith but unauthorized acquisition of personal information for lawful purposes is not considered a breach under Massachusetts's law unless the information is used in an unauthorized manner or subject to further unauthorized disclosure.

Confidential Information or "CI"
University Information that falls into one of the following categories:

a. Massachusetts Personal Information (as defined herein)

b. Financial Customer Information (as defined herein)

c. Records and information the University, or any of its employees or units, is required by law to keep confidential, including but not limited to the following:
    i. Personally identifiable information about students of the University, other than "directory information," contained in "Education Records," i.e. records "directly related to a student", to the extent protected by the federal law known as the Family Educational Rights and Privacy Act or "FERPA"
    ii. Records pertaining to individuals receiving health care related services from any Massachusetts licensed clinic operated by the University, to the extent they are considered confidential under Massachusetts law.
    iii. Information considered privileged under Massachusetts law, including but not limited to information consisting of or relating to communications between an individual and an employee of the University acting in their professional capacity as a licensed psychotherapist, psychologist, mental health counselor, or sexual assault counselors.

d. Information the University is required by contract, or by University policy, to keep confidential

e. Other highly sensitive personal information about an individual the disclosure of which could foreseeably result in identity theft, financial fraud, damage to reputation, or acute embarrassment, or other significant harm to the individual. Examples of such information include: information about a person's medical condition or physical or mental health or personnel or employee payroll records.

f. Other University Information that is proprietary to the University and that the University has a strong financial, strategic, or competitive interest in keeping confidential, or that the University is expected to keep confidential under applicable ethical norms. Examples of such information include: trade secret information, proprietary information relating to inventions or patents, research data, or personal information about volunteer research subjects collected in the course of human subject research.

Electronic
Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted
The transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Financial Customer Information or "FCI"
Personally identifiable information (that is not publicly available) pertaining to an individual that the University obtains in the process of or as a result of its offering or providing a financial product or service (e.g., student loans, financial aid applications and awards), and that is subject to the requirements of the GLB Regulations and is covered
in the definition of "personally identifiable financial information" in section 313(a) of those
Regulations (16 CFR 313(a)).

Examples include:

i. Information a consumer (including a student's parent) provides on an application to obtain a loan or other financial product or service;
ii. Account balance information, payment history, overdraft history, and credit or debit card purchase information;
iii. The fact that an individual is or has been one of the University's financial customers or has obtained a financial product or service from the University;
iv. Any information that a consumer provides to the University or that the University or its agent otherwise obtains in connection with collecting on, or servicing, a credit account;
v. Any information the University collects about a customer through an Internet "cookie" (an information collecting device from a web server); and

vi. Information from a consumer report (e.g., credit report).

GLB Regulations
The regulations of the Federal Trade Commission (FTC) codified at 16 CFR Part 314, entitled "Standards for Safeguarding Customer Information" which implement the financial customer information safeguarding requirements of the Graham-Leach-Bliley Act.

Internal Use Information
University Information that is less sensitive than Confidential Information, but that, if exposed to unauthorized parties, may have a possible adverse impact on personal interests, or on the finances, operations, or reputation of the University. Examples of this type of data from an institutional perspective include internal emails or memos meant for limited circulation, draft documents subject to internal comment prior to public release, or documents describing internal security procedures.

Massachusetts Personal Information or "MA Personal Information" or "MA PI"
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's: (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; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Massachusetts Regulations or "MA Regulations"
Regulations of the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) codified at 201 CMR 17.00, entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth"

Policy Manual
The Suffolk University Information Security Policy Manual referred to in section of this WISP.

Public Information
University Information that is required by law to made available to the public, or information other than Confidential Information or Internal Use Information that that University is not prohibited by law from making public and may in its discretion make public. Examples of this type of information include: press releases, reports sent to government agencies (other than confidential reports exempt from disclosure under federal FOIA or state Public Records laws), publicly posted class schedules, announcements distributed to the university community, and public listings of university events.

Record or Records
Any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Third Party Service Provider
Any person or entity that receives, maintains, possesses, or otherwise is permitted access to MA Personal Information or Financial Customer Information maintained by the University through its provision of services to the University; provided, however, that the term shall not include the United States Postal Service or other common carrier (e.g., Federal Express or the United Parcel Service).

University Information
Any information in any form whether electronic, hardcopy, audial, or otherwise which is created, collected, stored, accessed or used in connection with the operation and/or management of the University, or which is created, collected, stored, accessed or used by a party authorized by the University.

University Information Resource
Any tool, device, equipment, or system used to create, collect, record, process, store, retrieve, display and transmit University Information, including but not limited to email, mainframes, servers, computers, laptops, personal digital assistants (PDA), telecommunication resources, fax machines, printers, file cabinets, software and embedded technology.

University Users
All University faculty or staff members, whether full-time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the University, including any Third Party Service Provider providing services to the University who create, use or otherwise access or interact with any University Information and/or University Information Resource.

Administrative Oversight & Roles Responsibilities

Chief Information Officer

The University's Chief Information Officer (CIO) will create and oversee the WISP and review with the Information Security Officer (ISO) and to the extent needed, with the designated Department Information Security Coordinator (DISC) in each academic and administrative department at least annually or whenever there is a material change in business practices related to the WISP. The CIO will also oversee (and the ISO will implement) information security training in connection with the WISP to ensure that faculty, staff and administrators are aware of their responsibilities.

The CIO will also be, directly or through delegation and oversight, responsible for:

a. Overseeing the WISP, which includes the creation, implementation, compliance and ongoing review of the WISP and all related policies described in the University's Information Security Policy Manual.

b. Overseeing development of efficient operational procedures in support of the WISP;

c. Overseeing regular testing of the WISP safeguards;

d. In consultation with the CIO, the ISO and the DISCs in each of the University's academic or administrative departments, overseeing the process of identifying Confidential information (CI), assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing CI, ensuring the implementation of additional safeguards that are needed, performing periodic future evaluations of the continuing effectiveness of then-existing safeguards, and ensuring that the University's WISP contains all appropriate requirements, including, for example, controls to appropriately limit access to CI to individuals with a legitimate need for access, and policies relating to the proper disposal of records containing CI when such records are no longer necessary to accomplish the University's legitimate business purposes, and are not (or are no longer) required to be retained under state or federal law;

e. In consultation with the University's Office of General Counsel, evaluating the ability of Third Party Service Providers to comply with the MA Regulations, the GLB Regulations, and the WISP, in the handling of MA PI and FCI for which the University is responsible, ensuring that the University's contracts with those service providers include provisions obligating them to comply with those regulations and WISP requirements in providing the contracted-for services, or obtaining from such service providers written certification that they have a written, comprehensive information security program that is in compliance with the provisions of those regulations and requirements;

f. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing CI;

g. Assuring regular and appropriate training is provided to employees (and other University Users as appropriate) with access to CI;

h. Ensuring that any violations of the WISP are promptly corrected, and that appropriative action is taken to prevent similar violations in the future, and in consultation with Human Resources and the employee's supervisor or department chair or director, ensure that appropriate disciplinary action is taken against individuals responsible for the violations in appropriate cases;

i. Instituting a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or use of PI and FCI and for upgrading the WISP as necessary;

j. Ensuring that the WISP complies with applicable laws and the University's mission;

k. Designating the University's Information Security Officer;

l. Providing necessary resources to the ISO to ensure compliance with information security requirements; and

m. Oversees the ISO's audits of the WISP.

Information Security Officer

The ISO is directly or through delegation and oversight, responsible for:

a. Periodically conducting an internal audit of the WISP to validate controls, monitor systems and detect, prevent and mitigate any unauthorized use of or access to Confidential Information; and Monitoring compliance with the WISP;

b. Instituting a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or use of PI and FCI and for updating the WISP as necessary;

c. Jointly reviewing with the Office of General Counsel all third-party product or service contracts that relate to the collection, storage, use, transmittal or other access to Confidential Information;

d. Handling questions regarding information security, including those questions related to the WISP;

e. Developing and delivers ongoing, comprehensive training related to the WISP for all faculty, staff and administrators (and other University Users as appropriate);

f. Developing and implements a regular internal audit of the WISP Information, procedures and practices of the University; and

g. Supporting the CIO in annually reporting on the effectiveness of the WISP, including progress or remedial actions.

Department Information Security Coordinator(s)

A Department Information Security Coordinator (DISC) is identified by the appropriate
Dean or Vice President and is responsible for:

a. Conducting and documenting initial and periodic assessments to identify Records and University Information Resources that are maintained, accessed or used by the DISC's department;

b. Develops written procedures (in consultation with the CIO and ISO when necessary), concerning physical access to departmental Records, and the security and appropriate storage and maintenance of such Records;

c. Meets periodically upon request with the CIO and ISO to share information, coordinate implementation of the WISP and related University policies, and plan for and help deliver training to departmental faculty and staff.

Assessment of Internal and External Risks

The internal and external risks to the confidentiality, security and/or integrity of Records containing Confidential Information were assessed through a thorough, careful process which was led by the CIO, ISO, Assistant Provost for Regulatory Affairs, representatives from the various University departments that maintain or have access to Confidential Information, and numerous outside consultants. This assessment involved:

- Consideration of all relevant laws and regulations relating to Confidential Information, including the Massachusetts Regulations and the GLB Regulations;
- An evaluation and assessment of Suffolk University Records and information systems, and the physical, technical and administrative policies and safeguards built into those systems;
- A discussion with various University departments and other administrators of all potential internal and risks including but not limited to possible technological intrusions and security breaches caused by or resulting from individuals utilizing so-called viruses, worms, bots or other technological means to access, obtain, utilize, change or destroy the University's Confidential Information.

Looking forward, the University, led primarily by the CIO and ISO, will continue to assess external and internal risks periodically, and as changes to technology occur which may represent or introduce new kinds or degrees of risk.

Data Classification

Suffolk University Information is classified into the following types of information:

- Confidential Information (defined)
- Internal Use Information (defined)
- Public Information (defined)

Confidential Information Standards & Procedures

General Program Standards

a. Confidential Information must generally be protected to prevent unauthorized access, use, modification, transmission, storage or disclosure, and/or loss, or theft.

b. A copy of the WISP will be made available, and provided physically or electronically, to each University User with access to Confidential Information (CI).

c. Initial and periodic future training and retraining of employees (and other University Users as appropriate) with access to CI will be required by the University. All participants in such training sessions are required to certify their completion of the training.

d. All security measures shall be reviewed at least annually, or whenever there is a material change in the University's business practices that may reasonably implicate the security or integrity of Records containing PI or FCI. The CIO shall be responsible for overseeing this review and shall consider for implementation recommendations for improved security arising out of that review.

e. The ability of Third Party Service Providers to comply with the MA Regulations and the GLB Regulations (and the requirements of this WISP) in the handling of PI and FCI will be evaluated regularly and the University will ensure that contracts with those services providers will include

provisions obligating them to comply with the MA Regulations and the GLB Regulations (and the requirements of this WISP) in providing the contracted-for services.

Information Collection, Access and Use of Confidential Information

a. The amount of Confidential Information collected must be limited to that amount reasonably necessary to accomplish the University's legitimate educational and business purposes, or necessary to comply with other state or federal regulations.

b. Access to records containing Confidential Information shall, to the full extent feasible, be limited to those persons who are reasonably required to know such information in order to accomplish the University's legitimate educational and business purpose or to enable the University to comply with other state or federal regulations.

c. Electronic access to databases and files with Confidential Information will be blocked after multiple unsuccessful attempts to gain access have been attempted by the user when such access-blocking technologies are feasible and reasonably available.

d. Physical and electronic access to Confidential Information of a terminated or former University User shall be immediately blocked. Such terminated person shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the University's premises or information. Moreover, such terminated person's remote electronic access to Confidential Information shall be disabled and his/her voicemail access, email access, Internet access, and passwords shall be invalidated. The CIO and ISO shall maintain a highly secured master list of all passwords and encryption keys.

e. All terminated or former University Users who have (or had) access to Confidential Information shall be required to return all records containing Confidential Information, in any form, which may at the time of such termination be in the person's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

f. Access to electronically stored MA PI and FCI shall be electronically limited to those employees and other authorized University Users having a unique logon; and re-logon shall be required when a computer has been inactive for more than a few minutes.

g. There must be secure user authentication protocols in place, including:
    i. Protocols for control of user IDs and other identifiers;
    ii. A reasonably secure method of assigning unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access to PI or FCI
    iii. Restricting access to records and files containing personal information to those who need such information to perform their job duties.
    iv. Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
    v. Blocking of access to users after multiple unsuccessful attempts by those users to gain access.
    vi. Access to Confidential Information shall be restricted to active users and active user accounts only.
    vii. Passwords for current University Users shall be changed periodically in accordance with the "Password Policy".
    viii. All University-issued computers, including laptops, will be password protected and require a user name and password that complies with University policy.

h. All computer systems will be reasonably monitored for unauthorized use of or access to MA PI or FCI.

Storage and Maintenance of Confidential Information

a. University Users must maintain Records containing MA PI and FCI in locked facilities, secure storage areas or locked containers. Users are encouraged to store other Confidential Information in the same manner, although a somewhat lesser degree of physical security (e.g. storage in a filing cabinet in a limited access office which is locked during evenings and extended periods of non-attendance) shall normally suffice for Confidential Information that does not include MA PI or FCI.

b. University Users are prohibited from leaving open files (both electronic and paper) containing MA PI and FCI unattended. Records containing MA PI and FCI must be secured in locked file cabinets or locked drawers. and computers that have access to MA PI and FCI.

c. University Users with computer with access to PI and FCI shall be configured with automatic locking (requiring re-entry of a password) after a certain time of no activity, as specified in the "Password Policy".

d. At the direction of the DISC, each department shall conduct, and appropriately document, initial and periodic/subsequent assessments, to identify all of the Records and University Information Resources maintained, or accessed and used, by the department and to determine which contain Confidential Information. Each department shall also develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing Confidential Information are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted.

e. Confidential Information shall not be stored on any unencrypted laptops, handheld computers (e.g. IPads) or personal digital assistant (“PDA”) devices (e.g. Blackberry, I-Phone, Droid) or similar device, and shall not be stored on any unencrypted portable or removable storage media (e.g. CDs, flash drives, USB drives, external hard discs, etc.).

f. When stored in an electronic or other digital format, Confidential Information must be protected with Strong Passwords (See "Password Policy").

g. In those instances in which Records or media need to be temporarily transported, carried or stored outside of the workplace in connection with an employee’s University duties, they shall be held and stored in a secure fashion. For example, paper records shall be stored in a locked briefcase or file drawer whenever possible and/or shall be kept at all times within the physical custody of the responsible employee.

h. There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the Confidential Information installed on all systems connected to the internet which process Confidential Information.

i. 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 Confidential Information.

Transmission and Disclosure of Confidential Information

a. Any disclosure of Confidential Information outside of the University must be in accordance with law.

b. University Users are prohibited from sending any Records containing MA PI or FCI via email through the Suffolk Network, across public networks or wirelessly (whether to internal or external recipients)

unless such Records, messages or files are encrypted. University Users are also encouraged to refrain from sending any unencrypted records, messages or files containing Confidential Information via email through the Suffolk Network, across public networks or wirelessly (whether to internal or external recipients). In such instances, University Users are encouraged to find other more secure means of communicating such information (e.g., by providing a link to a confidential document stored on a secure University server, rather than an attach the document to the email message) whenever possible, especially in cases where the information in the document is particularly sensitive (e.g. where its unauthorized disclosure to external parties could foreseeably result in harm to an individual's reputation or other personal interests, could readily be used to perpetrate identity theft or financial fraud, or could foreseeably result in the loss of significant rights by, or financial damage to, the University or a third party doing business with the University).

c. Whenever performing University-related work involving Confidential Information, University Users should always use the University Computer Network and the University Virtual Private Network.

Information Retention and Disposal

a. Paper records containing MA PI or FCI shall be burned or shredded, and electronic records (including records stored on hard drives or other electronic media) shall be destroyed or erased, so that personal data cannot practicably be read or reconstructed. Other Confidential Information should be similarly shredded, destroyed or erased.

b. Record retention and disposal shall also be in accordance with the provisions of the Suffolk University Records Management Policy and related Record Retention Schedule.

c. It is expected that Records will be disposed of at the end of the applicable retention period(s) specified in the Suffolk University Records Retention Schedule. If a custodian of a Record, or group of Records, believes there is a legitimate business reason for retaining such Record(s) beyond the stated retention period, that custodian is expected to consult with CIO, who shall determine whether the Record(s) may or may not be retained for a longer period, and if so, for how much longer.

Internal Use Information Standards & Procedures

The following standards and procedures shall apply to Internal Use Information

Information Collection, Access and Use of Internal Use Information

a. Internal Use Information should be generally protected from any unauthorized access, modification, transmission or storage.

b. Internal Use Information is restricted to members of the University community who have a legitimate purpose for accessing such information.

Storage and Maintenance of Internal Use Information

a. Internal Use Information should be generally protected from any unauthorized storage.

b. When stored in any physical form (i.e., paper), Internal Use Information should be stored in a closed container to protect disclosure such as; filing cabinet, closed office, or desk drawer.

Transmission and Disclosure of Internal Use Information

a. Internal Use Information should be generally protected from any unauthorized transmission and disclosure.

b. Documents containing Internal Use Information should not be posted publicly.

Information Retention and Disposal

a. Documents containing Internal Use Information should be destroyed by shredding or an alternative process that destroys information beyond recognition or reconstruction (if in hard copy form), or should be sanitized or securely deleted by the Information Security Officer or his or her designee (if in electronic form) in accordance with the University's Record and Information Management Policy and Records Retention Schedule. (See Record Retention Policy)

Responses to Incidents and Breaches

- Employees and Third Party Service Providers with access to Confidential Information will be encouraged to report any suspicious or unauthorized use of Confidential Information in accordance with procedures described in the "Incident Response Policy" section of the Suffolk University Information Security Policy Manual.
- Whenever there is an information security related incident that constitutes a Security Breach involving MA PI and requires notification under M.G.L. c. 93H, §3, there shall be an immediate mandatory post-incident review of events and actions taken in accordance with the "Incident Response Policy". if any, with a view to determining whether any changes in security practices are required to improve the security of MA PI in accordance with the MA Regulations.

Incorporation of Other University Information Security Policies

This WISP includes, and incorporates by reference, the information security standards, polices, and procedures set forth in the Suffolk University Information Security Policy Manual, which includes the following:

- Acceptable Use Policy
- Anti-Virus Policy
- Encryption Policy
- Incident Response Policy
- Password Policy
- Portable Device Policy
- System Administrator Account Policy
- User Account Policy
- Vendor Policy

Waivers and Exceptions

Individuals subject to the mandatory requirements or standards set forth in this WISP, or the Information Security Policy Manual, may request that the CIO grant a waiver or exception from a particular requirement or standard that cannot practicably be followed without substantial operational hardship or excessive cost, and the CIO may in his/her discretion grant such waiver or exception provided that

a. the waiver or exception would not result in a violation of applicable law or regulation; and

b. that the CIO imposes, wherever possible, other alternative requirements or standards that serve the purposes of the WISP and/or Information Security Policy Manual but are less burdensome on the particular individual or his/her department or unit.

Enforcement and Disciplinary Action

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with the WISP. Violations of the WISP will result in appropriate disciplinary action, which may include temporary or permanent

restrictions on access to certain information or networks, or other employment related discipline up to and including suspension or termination of employment, depending on the circumstances and relevant factors such as the nature and severity of the violation and whether the violation was knowing, intentional or repeated.

Revision History

Version	Date	Responsible University Office	Approved By
1.0	09/14/10	Provost Office	Provost Barry Brown
1.1	02/12/13	Senior VP of Finance and Administration and Treasurer Office	Senior VP Danielle Manning