Northeastern University

Office of Information Security

Written Information Security Program (WISP)

1/1/2013

Northeastern University

Office of Information Security

Written Information Security Program (WISP)

1/1/2013

Table of Contents

Section 1: Administrative. Technical and Physical Controls to protect Personal Information

The University maintains administrative, technical and physical controls to protect Personal Information (Pii):

Administrative controls include, but are not limited to Appropriate Use Policy, Information Security Policy, marking of confidential information, security awareness training and communications, internal and external audit, and processes and procedures for granting and revoking access to physical and electronic forms of information.

Access to institutional information is based on need to know concept, where access to information is granted to those persons whose job duties and scope of employment creates a need to know.

Security practices are reviewed, modified and/or added based on academic, research, business needs, regulation, and evaluation of the threat landscape conducted by the Office of Information Security and Identity Services and allied functions.

Technical controls include but are not limited to perimeter firewalls, intrusion prevention systems, interior firewalls, encryption, authentication and authorization systems, system logging, file backup, virtual private network facilities, and network monitoring solutions.

Physical controls include but are not limited to electronic and physical card/key access control systems, locking mechanisms for areas and devices containing sensitive information and information-processing assets, creation of backup media, offsite storage of media, intrusion detection systems with central monitoring, closed circuit television monitoring and recording systems, fire detection, reporting and suppression systems, and water leak detection systems.

Section 2: Designated Responsibility for Information Protection

The University maintains a designated position responsible for information protection. This position is titled "Director of Information Security, and reports to the Vice President of Information Services. The position maintains the comprehensive information security program. In addition, certain colleges, business and research units have their own designated individuals who are assigned roles for information protection initiatives germane to their respective areas. The written information security program (WISP) is updated as needed and at least annually by the Director of Information Security

Section 3: Identification of paper, electronic and other records, computing systems, and storage media. including laptops and portable devices, that contain personal information

To the extent technically and operationally feasible, the University seeks to identify paper, electronic and other records, computing systems, and storage media, including laptops and portable devices that contain Pii.

Section 4: Identification of reasonably foreseeable internal risks to paper, electronic and other records containing Pii

The University continuously evaluates reasonably foreseeable internal risks to all forms of Pii. These evaluations are performed in the normal course of business and in cooperation with business and academic units across the University. Recommendations arising from these efforts are returned to the appropriate unit for consideration and implementation.

Section 5; Evaluation of current safeguards

The Office of Information Security routinely reviews existing information protection safeguards.

Section 6: Employee training

The University offers on-line security awareness training to all students, faculty, and staff. In addition, security education materials are publicly available on the Information Services website (www.infoservices.neu.edu) and through the Blackboard portal. Specially-prepared information security awareness and compliance trainings are made available as needed and/or as required to meet the special needs of business, academic, research and student groups.

Section 7: Procedures for monitoring Employee compliance with policy and procedure

All individuals applying for electronic access to Pii are responsible for familiarizing themselves with all University policies, which include handling and protection of sensitive information. This notice may be contained either in their application for an account, non-disclosure agreement, confidentiality agreement and/or notice printed on electronic account application forms and web pages.

Compliance with security procedures is monitored in the normal course of business by:

- ***Departmental officials,***
- ***Office of Information Security, and***
- ***Office of Networks and Telecommunications.***
- ***Compliance & Risk Services Department***

Violations of policy are managed using procedures outlined in Appendix A of this document.

Section 8: Means for detecting and preventing security system failures

Security systems are monitored continuously. Failures are reported to appropriate staff via event messages sent via email, pager, instant message or other forms of communication. Prevention of system failures is accomplished by implementation of fail-over systems, rigorous attention to maintaining all security systems with current operating system and application patches and fixes, and regular maintenance.

Section 9: Policy and procedure for when and how records containing Personal Information should be allowed to be kept, accessed or transported off the business premises

Records retention policies are promulgated by the Department Compliance and Risk Management Services. University policy creates procedures and technical standards for keeping, accessing and transporting personal information while on and off business premises.

Section 10; Blocking of physical and electronic access to records containing Personal Information

Centrally-issued computer accounts are deactivated by means of notification from Human Resources Management, the Office of the Registrar, special request through Office of Information Security, or accountholder sponsors. Each evening, identities of terminated individuals are sent to Information Systems, where automated and manual processes terminate access.

In urgent situations where access must be immediately terminated, a supervisor or other University official notifies the Office of Information Security. An electronic directive is then emailed to system administrators. The email specifies the account to be deleted and requests a confirmation message from each system administrator that an individual's account either has been deactivated, or does not exist on the resource for which the administrator is responsible.

Physical access to records is terminated by collection of keys and/or other access tokens used to access physical spaces, per policies of the Human Resources Department. In certain cases, incremental situation-specific safeguarding actions may be taken.

Section 11; Contracts with third party providers; Explicit requirement to maintain safeguards consistent with those in 201CMR 17.00

Third party service providers with whom the University may need to share Pii must be evaluated to determine whether they maintain safeguards and practices that provide for protection of Pii, consistent with the Massachusetts data breach regulations (201 CMR 17.00). Any University contract with a third party service provider must require that the service provider protect and maintain Pii consistent with Massachusetts data security regulations, including the existence of a Written Information Security Program (WISP). Third parties are asked to explain and verify how their information protection practices meet or exceed those required under the Massachusetts data security regulations.

The Commonwealth of Massachusetts publishes a 201CMR17.00 Compliance Checklist at: http://www.mass.gov/Eoca/docs/idtheft/compliance checklist.pdf The Compliance Checklist includes a checklist relative to topics that must be included in the Written Information Security Program (WISP).

Section 12; Amount of Pii collected and maintained; Limited to the amount reasonably necessary to accomplish legitimate business purposes, or to comply with state or federal regulations;

University information security policy requires the amount of Pii collected in any data collection experience, including paper and electronic experiences be limited to the minimum amount necessary to accomplish the legitimate academic and/or business need for which the Pii was collected.

Section 13; Procedure for documenting any actions taken in connection with any breach of security and post-incident review of events and actions taken to improve security.

The University maintains a Computer Security Incident Response Protocol and observes the FTC-mandated "Red Flags" protocol. As the Computer Security Incident Protocol is executed, contributors document actions taken and post-incident review to improve security where technically, operationally and financially feasible.

Section 14; Authentication and Authorization Protocols

User IDs and passwords to certain systems may be obtained by self-service by a proposed accountholder visiting a website and presenting information only the proposed accountholder would know. For certain other applications or systems, a formal paper or electronic application is required to be completed by an applicant and approved by management before access is granted.

Section 15; Methods of assigning/selecting passwords

Reasonably secure method of assigning/selecting passwords

In certain electronic experiences, accountholders self-create their password after providing information only the authentic person would know. Password construction rules are provided to the accountholder and technologically enforced within all centralized enterprise applications.

In other experiences, a candidate applies for access to as specific resource, and after a review process, the candidate may be granted a temporary password, or may be added to a group or role. The appropriate system administrator creates a password, which is sent to the Office of Information Security where the request is logged. The password is then transmitted to a secure location where authorized individuals notify the accountholder their password is ready for pickup. Accountholders personally appear to claim their password, where two forms of identification are required, one of which must be a government—issued photo ID. Accountholders are further instructed to change their password on first login.

In circumstances where an accountholder is unable to personally appear to claim their password, the password may be telephonically conferred after the candidate provides a set of identification information that matches University records. Passwords may also be conferred on paper by means of courier service to an applicant's address of record.

Section 16; Control of data security passwords

Passwords are kept in a location and/or format that does not compromise the security of the data they protect

Passwords are generated and maintained in secured areas at all times.

Section 17; Restricting access to Pii to active users and active user accounts

Electronic access to Pii is permitted on a need-to-know and scope-of-employment basis. The duration of time an account is active is limited to the duration of a person's role as reported by official University systems of record. Access is revoked automatically at termination of employment or engagement. Access can also be revoked on an emergency basis through the Office of Information Security.

Section 18; Blocking access after multiple unsuccessful attempts to gain access

Access to certain electronic resources is blocked after a history of unsuccessful attempts to gain access.

Section 19; Unique identifications and passwords

Unique user IDs and passwords are assigned to each accountholder. Password construction rules are designed to allow accountholders flexibility in creating a password designed to maintain the security of the secret.

Section 20: Encryption of Pii across public and wireless networks
University policy requires all Pii sent across public and/or unencrypted networks to be encrypted.

Section 21: Encryption of Pii on portable/removable devices
University policy requires that no Pii be stored on portable/removable devices, in instances where the business need demands it and an exception is granted, that it is suitably encrypted.

Section 22 Monitoring to alert on occurrence of unauthorized access
Monitoring for the occurrence of unauthorized access is applied to systems where it is technically, operationally and financially feasible to do so.

Section 23: Firewalls and operating system security patches
The University uses perimeter access control lists, firewalls and intrusion prevention systems. All University owned and managed devices are "patched" either automatically, or, in cases where unmanaged application of a patch may disrupt operations, patches may be applied manually.

Section 24: System security agent software
All University-owned and managed computers are automatically enrolled in update services for antivirus/malware protection.

Section 25: Employee training
The University offers Information Security Awareness training through the Blackboard Electronic Learning System. Training is available for all NU faculty staff and student employees.