Northeastern University

Office of Information Security and Identity Services

SSN and Personal Information Collection, Handling and Use Procedures

[Supersedes SSN Collection, Handling and Use Policy dated 3/7/07]

2/26/2010

Procedures	All handling and use of the Social Security Number (SSN) and Personal Identification Information (Pii), including disclosure to third parties and/or third party service providers, storage on removable devices, transmission on unencrypted networks and/or removal from University premises shall be limited to purposes required or permitted by law or regulation, and in matters of inquiry conducted by authorized University officials.

Definitions

Term	Meaning
Social Security Number (SSN)	A unique nine-digit number assigned to an individual by the United States Social Security Administration for purposes of revenue collection and disbursement.
Personal Information (Pii)	A Massachusetts resident's **First Name** and **last Name**, OR **First initial** and **last name**, ***AND*** one of more of the following data elements: - *Social Security Number (SSN)* - *Driver License number or state identification number* - *Credit and/or debit card number* - *Financial account 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*
Non-Pii Data	1. Information lawfully obtained from publicly available information, ***AND*** 2. Information obtained from federal, state or local governments, lawfully made available to the general public.
Need-to-know	Circumstance where an employee or authorized agent requires access to information in order to fulfill their assigned job duties.
Scope of employment	The complete range of activities an employee might reasonably be expected to perform while carrying out the business of the employer.

How SSN/Pii Information May Be Collected and Used

This TYPE of information…	May be collected and used for these PURPOSES…
Social Security Number (SSN)	1. Tax authority (IRS W-4), State agency reporting, Federal agency requirements (INS I-9), Federal, State and Private Parent and Student loan program processing, Federal and State Student Financial Aid Grant and Scholarship Processing, Student Employment Processing, Collections activity, Federal grant administration, Vendor payment controls, and subsequent collections as may be required to maintain compliance with local, state or Federal regulations. 2. Conduct of official University academic and administrative matters, where collection, handling and use of SSN is essential to provision of service to students, faculty, staff and affiliates.
Personal Identification Information (Pii)	1. Conduct of official University academic and administrative matters, where collection, handling and use of Pii is essential to provision of service to students, faculty, staff and affiliates.

Policy Violations • Enforcement/Audit • Remediation • Assistance Program

Failure to comply with these procedures may constitute a violation of University policy and may subject the violator to disciplinary action by the University. Training is available to departments periodically and on request,

Databases, Documents and Feeds

Databases and documents containing SSN where presence of SSN is not required or permitted shall have been purged of such information by June 1, 2007.

SSN may not be obtained by manual or electronic feed, except only for purposes required or permitted by law or regulation. Electronic content containing SSN and/or Pii shall be protected from unauthorized access using reasonable administrative, physical and technical safeguards.

Proposed New Collection, Storage or Uses of SSN/Pii

All newly-proposed collection, storage, uses, transmission of SSN and/or Pii; including system changes, unless such activities are required or permitted by law or regulation, are subject to prior review and approval by the Provost or their designee.

Service May Not Be Conditioned on Collection of Social Security Number (SSN)

The University may not condition any service or transaction on collection of SSN except only as may be required to resolve identity where no other means is available nor conclusive, or as may be required or permitted by law or regulation. The University may collect SSN and/or Pii to the extent required to positively identify an individual in order to conduct or complete an academic or business transaction, or in the conduct of an official investigation under the auspices of authorized University officials.

Collection and Maintenance of Personal Identification Information (Pii)

Collection and maintenance of Pii shall be limited to the minimum amount and time necessary to fulfill the legitimate purpose for which the Pii is collected. Pii may be maintained only for the minimum amount of time necessary to fulfill the legitimate purpose for which the Pii was collected.

Conversion Tables for SSN Use

Systems where SSN use is permitted may automatically cross-reference between SSN and other identifying information through use of conversion tables within the system, or by other technical means. All such conversion mechanisms and tables shall be owned, managed and maintained by the Information Systems organization.

Posting of Personal Information to Public Networks or Sites

SSN and/or Pii data of members of the Northeastern community, including but not limited to students, faculty and staff may not be posted nor maintained on public networks or sites, unless the user fully complies with applicable laws and regulations governing handling of personal information.

Part 12

Storage of SSN and/or Pii on Computing Devices

SSN and Pii records may be stored on University-owned devices to the extent necessary to facilitate assigned work that falls under need-to-know and scope of employment rules.

Part 13

Use of Safeguards

Certain information types are required to be protected with specific safeguards. The following table describes safeguards required for each type of information.

This INFORMATION TYPE…	Must be protected using these SAFEGUARDS…
Paper Documents, Printing and Display	Paper forms on which SSN and/or Pii is collected and/or stored shall be stored in locked containers or areas, and may be made available only to those who have a need to know the information. All paper forms bearing SSN and/or Pii shall be securely destroyed at the conclusion of need or expiration of the appropriate record retention period, whichever occurs first. Document disposal shall be performed in accordance with published Information Disposal Recommendations. These recommendations can be read at: http://www.infoservices.neu.edu/get_help/content/Info_Disposal_111409.pdf Devices used for display and printing of SSN and/or Pii shall be located and equipped such that only authorized individuals are able to view the output or display. Printed matter containing SSN and/or Pii shall be promptly removed from all devices on which such records are reproduced. **SSN, Pii, and/or student identification numbers shall not be used to post grades.**

Use of Safeguards (continued)

This INFORMATION TYPE…	Must be protected using these SAFEGUARDS…
Fax and E-mail	The nine-digit SSN and/or Pii shall not be shown on any email or fax message, except only when said transmissions are made solely inside University-owned networks or where the content is encrypted. If encryption is not feasible or available, all SSN and Pii data shall be redacted, truncated or reduced such that the data no longer meets the definition of Pii. For fax transmissions required by law or regulation, the sender shall verify the destination fax number prior to faxing, and shall obtain oral or email confirmation of fax receipt from the receiver. In all cases where confirmation of receipt is not obtained from the intended receiver, the sender must immediately notify the Office of Information Security and Identity Services at itsecurity@neu.edu, and provide the following information: 1. *Date fax or email was sent.* 2. *Sender name, title, office location, and origin/destination fax numbers.* 3. *Name of organization to which the fax or email was sent.* 4. *Name and email address of person to whom the fax or email was addressed.* 5. *Copies of materials faxed.*
Storage of SSN and/or Pii on Paper, Fiche, Optical and All Other Non-Electronic Media	Physical records of all descriptions containing SSN and/or Pii data shall be safeguarded under lock and key or other appropriate access control solution. Access to such records shall be limited to those who have a need to know, and/or whose scope of employment requires them to access the information.
Removal of SSN and/or Pii Data from University-Owned Premises	Electronic SSN and/or Pii data shall not be removed from University premises unless the data are encrypted, and provided removal of records is necessary, lawful, within scope of employment or role, and authorized in writing by the applicable department head.
SSN/Pii Stored on Laptop Computers and Removable Devices of All Descriptions	Locking devices and encryption shall be used on all portable/removable devices on which SSN and/or Pii is stored. **Only SSN and Pii data elements require encryption.** ***Other data elements are not required to be encrypted.***
Devices Through Which SSN/Pii is Accessible	Devices through which SSN/Pii is accessible must have password-protection engaged and the screen locked with a password at all times while unattended.
Disposition of storage devices containing SSN and/or Pii Data	Storage devices containing SSN and/or Pii data shall be dispositioned according to published Asset Disposition Procedures; available at the following link: http://www.northeastern.edu/facilities/adf1.pdf

Training

All new employees whose assigned duties include collection, handling, possession or transmission of SSN and/or Pii data shall undergo Information Security Awareness Training at the first class offered after start of employment or engagement. Training is given electronically via the Blackboard Electronic Learning system. It is the responsibility of department and unit heads to require their employees and service party providers to complete training. Individuals involved in SSN/Pii disclosure incidents shall undergo remedial Information Security Awareness Training

Part 15

Incident management

All suspected or actual breaches of SSN/Pii data, including suspected or actual theft of paper, electronic or technology devices on which SSN/Pii may have been stored, shall be immediately reported to the immediate supervisor, to the Office of Information Security at itsecurity@neu.edu, and to the Public Safety Division (x2696).

The Office of Information Security shall, in collaboration with appropriate University officials, determine the timing and process of written notifications of SSN/Pii data security breaches to each person whose data was breached. All notifications to affected individuals shall be sent from and signed by the Director of Information Securwity and Identity Services or their designate.

Redress

Any member of the NU community who feels their SSN and/or Pii data has been collected, handled or used contrary to this policy and/or state law may seek redress by contacting the Office of Information Security and Identity Services at itsecurity@neu.edu. When seeking redress, the following items of information are required:

- **Name and role at the University,**
- **Contact information (postal address & phone number),**
- **E- mail address, Date of occurrence, Description of concern, and**
- **Names and dates of contacts with of other University officials.**