

# SSN Collection, Handling and Use Policy

3/7/07

## General Policy Statement

On and after June 1, 2007, all collection, handling and use of the Social Security Number (SSN), including disclosure to third parties, shall be limited to purposes required or permitted by law or regulation, and in matters of inquiry conducted by authorized University officials. In general, SSN may be collected and used for the following purposes:

*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.*

Additionally, all means of handling SSN shall be subject to mandatory use of safeguards described in the policy.

## Policy Violations • Enforcement/Audit • Remediation • Assistance Program

Failure to comply with this policy shall constitute a violation of University policy and will subject the violator to disciplinary action by the University up to and including termination of employment or relationship, and may result in legal action.

The SSN Collection, Handling and Use Policy is enforced by the Office of Information Security and Identity Services, and Office of Internal Audit, in cooperation with appropriate University officials. Compliance audits may be conducted at any time, with or without notice. Departments are required to cooperate with all inquiries made in connection with this policy.

Non-compliance shall be promptly remediated by the appropriate system, process or record holder(s). An assistance program shall be available to qualified entities.

## Databases, Documents and Feeds

Databases and documents containing SSN, where presence is SSN is not required or permitted by law or regulation, shall be purged of SSN or converted to NUID prior to the June 1 deadline. Extension of the deadline for individual cases is at the discretion of the Senior Vice President for Finance and Administration.

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 shall be protected from unauthorized access using reasonable administrative, physical and technical safeguards.

## Service May Not Be Conditioned on Collection of SSN

No service or transaction may be conditioned on collection of SSN, except only as may be required to resolve identity where no other means is available or conclusive, or as may be required or permitted by law or regulation

### **Conversion Tables**

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.

### **Paper Documents, Printing and Display**

Paper forms on which SSN 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 SSN. All paper forms bearing SSN shall be securely destroyed at the conclusion of need or expiration of the appropriate record retention period, whichever occurs first. Document disposal shall be in accordance published Information Disposal Recommendations.

Devices used for display and printing of SSN shall be located in non-public areas, where only authorized individuals have access to the device and it's output. Printed matter containing SSN shall be promptly removed from all devices on which such records are reproduced, and paper copies shall be stored in locked containers or areas. SSN shall not be used to post grades.

### **Proposed New Collection, Storage or Uses of SSN**

On and after June 1, 2007, all newly-proposed collection, storage, uses, transmission of SSN, including system changes, unless such activities are required or permitted by law or regulation, are subject to prior review and approval of the Senior Vice President for Finance and Administration.

### **Fax and E-mail**

The nine-digit SSN shall not be shown on any fax transmission, nor shall SSN be sent via email, except only when said message is encrypted. If encryption is not feasible or available, all SSNs shall be reduced to the last four digits. For fax transmissions necessitated under law or regulation, the sender shall verify the destination fax number prior to faxing, shall obtain oral or email confirmation of fax receipt from the receiver.

### **Workstations and Laptop Computers • Removal of Records Containing SSN Written Authorizations Required**

SSNs belonging to members of the University community shall not be stored on personally-owned devices of any description, nor shall SSN be downloaded to or stored on University-owned home computers or devices.

Electronic or physical records containing SSN shall not be removed from University-owned facilities, unless such removal is lawful, within scope of employment or role, and is authorized in writing by the appropriate Vice President

Written authorizations for the foregoing shall identify the record(s) to be removed, the means of removal (paper or electronic), the date of removal, the name and contact information for the person taking possession, and the reason for possession. Approval shall be signed by both the supervisor and subordinate, and shall be retained by the relevant department. Approval records shall be produced on request from the Office of Information Security or internal/external audit functions.

Locking devices shall be used on all devices on which SSN is stored. Devices through which SSN is accessible must be password-protected at all times while unattended.

### **Disposition of storage devices containing SSN**

Storage devices containing SSN shall be dispositioned according to published Asset Disposition Procedures.

### **Training**

All new employees, agents or contractors whose assigned duties include collection, handling, possession or transmission of SSN, shall undergo Information Security Awareness Training at the first class offered after the start of employment or assigned role. Individuals shown to have been involved in SSN disclosure incidents shall undergo remedial Information Security Awareness Training.

### **Incident management**

All suspected or actual breaches of SSN security, handling or policy, including suspected or actual theft of paper, electronic or technology devices on which SSN may have been stored, shall be immediately reported to the immediate supervisor, and to the Office of Information Security at [itsecurity@neu.edu](mailto:itsecurity@neu.edu).

SSN security breaches shall promptly be disclosed in writing, to each person whose SSN was breached. The Office of Information Security shall, in collaboration with appropriate University officials, determine the timing, process and content of written customer notifications. All notifications shall be sent from and signed by the Director of Information Security and Identity Services, or their designate, except only as may be required where local, state or federal regulations pre-empt such action.

### **Redress**

Any member of the community who feels their Social Security Number has been collected, handled or used contrary to the policy may seek redress by contacting the Office of Information Security and Identity Services at [itsecurity@neu.edu](mailto: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