University of Wisconsin-Milwaukee
Information Assurance Protocol
for Social Security Numbers (SSNs)

March 2010

Audience

* All faculty, staff and students
* All employees, both permanent and temporary
* All contractors, vendors and any others (including 3rd parties) entrusted with SSN information.

Purpose

The University of Wisconsin-Milwaukee is required by University policy and state law\(^1\) to protect the SSNs that it stores or transmits from unauthorized access, disclosure or other misuse. Pursuant to UW-Milwaukee Information Security Policy S-59\(^2\), this protocol establishes campus-wide procedures and safeguards to control the risks involved in storing and transmitting SSN data.

Protocol Statement

SSNs should not be captured, retained, communicated, transmitted, displayed or printed, in whole or in part, except when required or permitted by law and where no other reasonable alternative exists.

SSNs may not be used as the primary identifier for any individual. Another unique identifier must be used.

Scope

In Scope:
The protocol applies to the SSN, whether maintained, used or displayed in any data format, including but not limited to, oral or written words, screen display, electronic transmission, stored electronic media, printed material, facsimile or other human or machine-readable medium.

Out of Scope:
Instances where only the last four digits of the SSN are stored or transmitted to verify an identity are out of scope.

Roles and Responsibilities

Data Custodians: Data custodians must develop processes and procedures to comply with this policy and must be provided the opportunity to approve or deny uses of and access to SSN information in their care.

UWM Human Resources and Business & Financial Services is the data custodian for all SSNs recorded, stored or transmitted for the purposes of employment and compensation of employees.

UWM Enrollment Services and Graduate Student Services are the data custodians for all SSNs recorded, stored or transmitted for the purpose of provisioning educational services and records.

UWM Financial Aid, Student Employment and Military Education Benefits are the data custodians for all SSNs recorded, stored or transmitted for the purposes of administering financial assistance.
Individual Researchers are the data custodians for SSN records, which they possess for research purposes.

SSNs collected, maintained or transmitted as part of University business not covered in the categories named above are the responsibility of the director of the area conducting the business requiring the use of the SSN credential.

Other Roles

Information Security:
Information Security develops and distributes standards for data protection.

Internal Audit, IT Systems Auditor:
Commensurate with risk, Internal Audit audits areas storing and transmitting the SSN credential to verify that standards have been implemented to protect the data from reasonably foreseen risks.

Protocol Requirements

1. Except when required or permitted by law and where no other reasonable alternative exists, the SSN may not be used as the primary identifier for any person in any system. A separate unique identifier will be used for employees and students in all future electronic and paper data systems and processes to identify, track, and provide service to individuals associated with the University. The non-SSN identifier will be permanently and uniquely associated with the individual to whom it is originally assigned.

2. Individuals shall not be required to provide their SSN, verbally or in writing, at any point of service, nor shall they be denied access to those services should they refuse to provide a SSN, except where the collection of SSN is required by federal law, or was required by State law or University policy in effect prior to January 1, 1975. Individuals may volunteer their SSN if they wish as an alternate means for locating a record.

3. Campus entities or their representatives will assess where SSN records exist, will to the extent possible remove SSN records, which do not meet the above criteria, and will secure the data, which is authorized for storage and transmission per University standards.

4. Approved technical, administrative and physical security safeguard standards are to be made available by UWM Information Security in conjunction with the UWM Internal Audit Information Systems Auditor. These will be publicly disseminated and updated as necessary. Any use of SSNs will be secured in compliance with these standards.

5. Data and document retention should adhere to standards set by state and University data retention policies. When disposal is appropriate, paper documents and electronic media containing SSNs will be destroyed or disposed of using methods approved by the UWM Archivist in conjunction with Information Security and Internal Audit designed to prevent disclosure of the information.

6. SSNs will not be released to entities outside the University except where necessary for providing educational services, financial aid, to perform background checks on existing or potential employees, or to meet legal requirements such as tax reporting or other government required activities.

7. Within the University, access to SSNs will be limited to those individuals requiring access as determined by job function, which directly supports legally required SSN use, storage and transmission. Written approval by the data custodians defined in the Roles and Responsibilities section of this document will be obtained prior to granting access to SSNs.
8. Individuals permitted access to SSNs will be instructed on the appropriate handling and protection of this data by their management or designated representative based on the standards set by Information Security in conjunction with Internal Audit. They will be offered training as appropriate, along with regular updates and reminders regarding their role in information security and privacy assurance.

9. Individuals with authorized access may not redistribute the SSNs without authorization from the data custodian.

10. UWM Internal Audit or their designate will review SSN access commensurate with risk.

12. All members of the University are expected to report any breach of privacy or security of SSNs should they become aware of such an incident.

12. A Privacy Act of 1974 Statement must be prominently displayed on any form, online or paper, which asks for an individual’s SSN.

Footnotes:


3. UW Milwaukee Confidential Data Protection Standards http://security.uwm.edu


5. Sample Privacy Act of 1974 Statement:

“The Privacy Act of 1974 requires that individuals providing their SSN in this form be informed of the authority which allows the solicitation of the SSN and whether disclosure of the SSN is mandatory or voluntary; and what uses will be made of the SSN.

The SSN in this form is being collected pursuant to [cite law allowing or requiring collection] and submission is [voluntary/mandatory]. The SSN is being collected for the purpose of [describe purpose]."