

Information Security Policy and Standards: Secure Handling of Social Security Numbers

Audience:

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

Definition:

It is Wheeling Jesuit University's intent to protect the personal information of its students, staff, administrators, and faculty and other individuals associated with the University from unauthorized access or disclosure, and possible misuse or abuse. This policy is designed to establish awareness and provide guidance on the proper handling of Social Security Number (SSN) information maintained by or on behalf of Wheeling Jesuit University.

Policy Statement:

Social Security Numbers may not be captured, retained, communicated, transmitted, displayed or printed in whole or in part, except where required or permitted by law, and in accordance with the standards outlined in this policy.

Background Issues:

Scope

The policy applies to the SSN whether maintained, used or displayed wholly or in part, and in any data format, including but not limited to oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or other medium as determined.

Policy Owner

Information Technology Services

References

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)

Definitions

1. Social Security Number (SSN) may be interpreted to include Taxpayer Identity Number (TIN).
2. Individual Workstations: Includes but is not limited to desktops, laptops and PDAs, and cell phones.
3. Removable or Transportable Media: Includes but is not limited to paper forms, reports, cassettes, CDs, USB tokens, flash drives, hard drives and zip drives.

Standards

1. Going forward, the University does not permit the use of a SSN as the primary identifier for any person or entity in any system, except where the SSN is required or permitted by law, and permitted by University policy.
2. Where required or permitted by law and University policy, the SSN may be stored as a confidential attribute associated with an individual or may be used as an optional key to identify individuals for whom a primary identifier is not known.
3. Individuals shall not be required to provide their Social Security number, 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 law or otherwise permitted by University policy.
4. Except where the SSN is required by law, the University ID (EMPLID) replaces use of the SSN and will be used in all future electronic and paper data systems and processes to identify, track, and service individuals associated with the University. The University ID will be permanently and uniquely associated with the individual to whom it is originally assigned.
5. All newly developed or acquired application software will not store SSN as a data element until a business requirement is submitted and approved by the Executive Vice President and/or other authorities as deemed appropriate.
6. Servers housing databases or records containing SSNs should be of single purpose, with access restricted to system administrators, protected by an approved firewall appliance, and should not be used by individuals to access the Internet or access e-mail.
7. Where possible, all records containing an SSN should be stored on network drives with access limited to those individuals or entities that require access to perform a legitimate University job function. Individual workstations, laptops and other personal computers (PDAs) should not be used to store records containing SSNs.
8. All removable or transportable media (e.g., paper forms, reports, cassettes, CDs, USB drives, etc.) containing SSNs must be secured when not in use. Reasonable security measures depend on the circumstances, but may include locked file rooms, desks and cabinets.
9. Subject to applicable document retention policies or unless required by law, when no longer required, paper documents and electronic media containing SSNs will be destroyed or disposed of using methods designed to prevent subsequent use or recovery of information.
10. SSNs will be released to entities outside the University only where permitted or required by law, or with the express written permission of the individual or entity, or where approved by General Counsel.
11. The University will limit access to records containing SSN to those individuals requiring access as determined by job function. Individuals permitted access to SSN will be instructed on the appropriate handling and protection of this data by their management or designated representative.

Procedure

Individual business units are responsible for the development, documentation and implementation of applicable procedures to effectuate this policy. Procedures are subject to review by appropriate division heads.

Compliance

All parties as delineated under Audience are required to comply with this policy no later than sixty days after approval (see "Date Effective.") Individuals who discover or strongly suspect the unauthorized release of SSN or related information, or a violation of this policy must promptly notify their management and any of the following:

- Information Technology Services 304-243-8181
- E-mail: security@wju.edu

Non-compliance: Any violation of this policy may be cause for appropriate disciplinary action, including dismissal.

Exception Process

Any request for exception to this policy should be submitted to Information Technology Services using the Exception Request Form attached to this document. ITS will coordinate requests for exception to this policy and contact the respective policy owner, and other authorities as deemed appropriate for consideration and discussion of the exception

request. Request forms must be completed fully; incomplete forms will be returned without processing. Requestors will be provided with a decision within ten (10) working days from receipt of the completed request.

Approved Uses of SSN

University offices may not collect SSNs for purposes other than those noted below. Any office intending other use of SSN data must request an exception to the policy (see Exception Process described above).

The primary uses and reasons for the continued capture, storage, retention and processing of SSN data are identified and documented in the Approved Uses of SSNs section described below. Typically, processes that access historical SSN data, or require or permit continued use of SSN data, are described here. Additional processes may be added to the appendix by contacting Information Technology Services.

The primary uses and reasons for collecting a SSN include the following:

- **Enrollment:** Any student applying for Financial Aid or Student Loans must provide a SSN to the University. If a person enrolling in a Wheeling Jesuit University academic offering - credit or non-credit - refuses to provide a SSN, certain services, such as transcripts, enrollment verification, tax reporting, financial aid and other services may not be available to the individual, and Wheeling Jesuit University cannot guarantee a complete academic record for the individual.

Historic hardcopy academic records may contain a student's SSN, as SSN was previously used as the student ID.

- **Employment (including student worker):** A SSN must be provided on I-9's in accordance with the Immigration Reform and Control Act of 1986 (IRCA), as overseen by Human Resources and or the WJU Business Office.
- **Any person employed by the University must provide a SSN as the taxpayer ID number as directed by the IRS.** This includes all employees, including part-time and student employees. Providing the SSN is a condition of employment. Applicants for employment must also provide a SSN, if requested, for mandatory background checks.
- **Employee Benefits:** If required by a benefits provider, the SSNs of dependents/beneficiaries may be collected to receive service. Wheeling Jesuit University may also release an employee's SSN to benefit providers.

Payment for Personal or Professional Services: Any person providing services to the University as a independent contractor, invited speaker (honorarium) or research subject for which payment will be made, must provide a SSN as the taxpayer ID number per IRS regulations. These taxpayer ID numbers will be stored in the accounts payable system as part of the vendor record.

- **Planned Giving Donors:** Donors participating in planned giving programs must provide a SSN as the taxpayer ID per IRS regulations.
- **Insurance Providers:** The SSNs of faculty, staff and students continue to be the patient identifier for many health care providers.
- **Office of Alumni Relations and Development (OARD):** The Office retains the student records of alumni.
- **Student Health Services:** The department requires and uses SSN as a primary identifier within its systems, due in large part to the required interaction with insurance companies
- **University Security:** Department personnel collect SSN data during an arrest as required by the West Virginia State Police and Federal Bureau of Investigation (FBI).

Secure Handling of Social Security Numbers Policy Exception Request

Name of Requestor:

Date:

Dept:

Phone:

Address:

E-mail:

Describe the type of media to be used to retain Social Security Number, e.g, Excel spreadsheet, database files, paper document, harddrive, etc.

If appropriate, explain why the Social Security Number must be retained electronically.

Where will the media be stored, e.g., a local PC, departmental server, file room, etc.?

How long will the media be retained?

Are data and backup data encrypted?

Will the Social Security Number be used as the primary identifier?

Estimate the number of records that will be retained.

List the approximate number of those individuals that require access to the SSN information retained by this system: Faculty Staff Admin Students Other

Describe the method(s) used to access the data e.g., from University IP address only, remotely via VPN, dial-up, etc.

Describe any access controls or security measures (e.g., firewall, physical security, encryption, etc.) that are or will be implemented to protect the data.

Please remit to Dan Feeley, Assoc. VP for IT for approval

Note: Incomplete request forms will be returned without processing. Requestors will be provided with a decision within 10 working days from receipt of the completed request.