Policy on Social Security Numbers

No. 1060

Policy Effective Date:
5/25/2007

Last Revision Date:
4/23/2021

Policy Owner:
Amy Sebring

Policy Author: *(Contact Person)*
Ken Miller

Affected Parties:
Undergraduate
Graduate
Faculty
Staff
Other

1.0 Purpose

Virginia Tech is committed to ensuring the privacy and proper handling of the *Social Security number* and the Individual Taxpayer Identification Number (collectively abbreviated as "SSN") that is collected to carry out its mission. The purpose of this policy is to ensure that university employees and offices comply with federal and state laws and regulations that affect the use of SSNs. Mandatory collection of SSNs will only be for purposes where the collection is mandated by a United States federal government agency or by the Commonwealth of Virginia.

Objectives of this policy include:

1. Consistent requirements regarding the usage and storage of SSNs throughout the university;
2. Awareness of the confidential nature of the SSN;
3. Minimized reliance upon the SSN for identification purposes; and
4. Increased confidence by students, employees, customers, and research participants that SSNs are handled in a confidential and secure manner by the university.

2.0 Policy

Virginia Tech's policy for handling SSNs includes the following:

- to collect SSNs when legally required or legally permitted and necessary to conduct university business;
- to access SSNs to conduct university business relevant to those legal requirements or business needs, including ensuring data security;
- to maintain SSNs securely; and
- to disclose SSNs only when legally permitted;
- this policy applies to faculty, staff, students, and external entities acting as university contractor or agent of the university.

2.1 Collection and Storage of SSNs

In accordance with the Virginia Government Data Collection and Dissemination Practices Act, unless disclosure is required by federal or state law, the university will not require individuals to provide their SSN for any purpose or in connection with any activity, or refuse any service because the individual does not disclose or furnish their SSN.

Approval of the collection and use of SSNs for university operations in accordance with the guidelines established in this policy resides with the Vice President for Finance, except in circumstances where they are collected and used for research purposes. Approval of the collection and use of SSNs for research purposes resides with the Institution Review Board (IRB). Data trustees and data stewards, as defined in Policy 7100, Administrative Data Management and Access Policy, have key roles in the implementation of this policy.

Data trustees must submit a written request for approval to the Vice President for Finance stating the legal requirement or business need for collecting the SSN and related processes in place to ensure the security of the SSN. Data trustees are defined in Section 3.1 for the purposes of the SSN policy as those Vice Presidents and Vice Provosts (VPs) who have oversight responsibilities for offices and functions that collect and/or report the SSN, and the Vice President for Information Technology & Chief Information Officer, who has oversight responsibilities for the storage of the SSN in enterprise databases.

Data stewards are defined in Section 3.2 as the managers of the operational departments where processes require the university to collect, store, and use the SSN.

2.1.1 Research Activities Collecting SSNs

Approval of the collection and use of SSNs for research in accordance with the guidelines established in this policy resides with the Institution Review Board (IRB) and is overseen by the Vice President for Research and Innovation. Data Trustees and Data Stewards, as defined in this policy, have key roles in the implementation of this policy.

Investigators must include a Data Management Plan (DMP) for the security of SSNs in their research protocol. The protocol must specify how the SSN collection is relevant to the research purpose. Disclosure of the SSN is required for completion of the IRS Form W-9 or Form W-8BEN when compensation exceeds $75. SSNs shall not be collected until the need has been clearly documented and approved by the IRB. The SSN may not be used for any purpose other than the purpose approved. The IRB will document the justification for collection of the SSN and whether disclosure of the SSN is voluntary or required for participation in the research.

Investigators are expected to collect and store SSNs in any media (electronic or paper-based) using appropriate security measures as documented in the study protocol. No study-related information may be stored with SSNs. SSNs must be maintained until final disposition using proper safeguards as provided in Virginia Tech information security (Standard for administrative data management, and Standards for high-risk digital data protection) and IRB guidelines. Department or Institute IT must attest that the DMP is accurate and that the environment provides the required protections.

SSNs may not be shared in external collaborations without the express authorization of the IRB and the research data steward.

2.1.2 Requests at Points of Service for SSNs

The SSN is assigned by the United States government and is subject to corrections brought to the attention of the university either by the federal government or by the individual to whom it is assigned. Virginia Tech may also undertake actions to verify SSNs.

When SSNs are being collected for operational purposes, different forms or levels of initial collection and verification may be required. For example, employment may require producing the Social Security card and/or verification of the number with the Social Security Administration, while compliance with the Taxpayer Relief Act permits reporting of the SSN by the individual student.

All university forms and documents used to collect SSNs will include a disclosure statement informing the reason to collect the information and will include language indicating whether the request is mandatory or voluntary. All university forms and documents that are used to collect SSNs will employ the language included in Section 4 of this policy. Forms and documents may also request voluntary disclosure at early stages of a process where the SSN is likely to be required of the individual at a later point in the process (for example, application for admission

or employment). These forms and documents must indicate that the request is voluntary at this stage, but may be required at a later stage in the process. Voluntary disclosure of SSNs will not lessen the need for appropriate safeguards.

2.1.3 Access to SSNs

Once collected, an individual's SSN will be stored only in locations needed to conduct university related business or approved research and will be accessed only for the purpose of conducting university related business or approved research.

Only authorized Virginia Tech employees and approved external entities acting on behalf of the university, who have a need to know the SSN may have access to it. Contractual agreements with external entities acting as the university contractor or agent requiring the sharing and disclosure of the SSN must be in writing. The written agreement must prohibit the disclosure of the SSN, except as required by law; must specify how the SSN will be used, and the services that the external entity will provide on behalf of the university requiring access to the SSN; and, require the external entity to use adequate administrative and technological safeguards to protect the confidentiality of the SSN.

2.2 Use of Collected SSNs

2.2.1 Use as Identifiers

SSNs will not be used either as identifiers of individuals nor as keys to records pertaining to individuals within databases. Virginia Tech employees, students, and other individuals who require a unique identifier will be assigned an identifying character string, called the *Virginia Tech ID number* (VT ID number). The VT ID number will not be the same as, nor derived from, the SSN.

2.2.2 Display and Dissemination of SSNs

University employees must exercise utmost care in maintaining the confidentiality of the SSN. SSNs, in whole or in part, must never be placed within public view.

SSNs may be released by the university to entities outside the university after approval for each instance by the IT Security Officer when:

- It is required to comply with government reporting and transactional mandates, or otherwise required by law; or
- Permission is granted by the individual; or
- The external entity is acting as the university's contractor or agent; or
- Pursuant to an authorized data transfer agreement.

When SSNs are released to external entities acting as contractor or agent of the university, the appropriate data steward is responsible to obtain satisfactory assurances that the information is held securely and is not re-distributed. Refer to Section 2.1.2 above regarding third-party arrangements.

Particular care must be taken with older records to prevent inadvertent, inappropriate release of SSNs.

2.3 Secure Storage and Transmission of the SSN

The SSN is considered high-risk information according to the Virginia Standard for High Risk Digital Data Protection. Departments are required to eliminate the unencrypted storage of SSNs in local databases, desktops or laptop computers. Departments or individuals with a business need to maintain SSNs must strictly adhere to the information security standards and policies. Please refer to the IT policies and standards for detailed information on data management policies including data risk classification, standards for administrative data management, and standards for high-risk digital data protection.

When paper documents containing SSN are sent through a delivery system (i.e., campus mail, U.S. Postal Service, messenger services), the documents must be appropriately safeguarded and marked confidential.

All digital records that contain SSN must be stored securely using standard encryption techniques. Electronic transmission of SSNs must follow established electronic transmission security standards (see Section 2.3.1 below). Data stewards and all data users of the SSN are responsible for ensuring proper and secure handling and disposition of both paper and electronic documents or files containing SSN in Policy 2000, Management of University Records.

2.3.1 Security Standards for SSN Maintenance and Destruction

Records (electronic and paper-based) which contain SSNs shall be maintained in a secure manner and in accordance with the university's records management procedures and record retention schedule. Paper forms or documents requiring SSN for university operations must be stored in locked rooms or cabinets. Information Technology Security Office (ITSO) maintains standards to address the electronic storage and transmission of SSNs. Adherence to these standards is required.

Upon reaching the end of the required retention period or no longer needed for business, approved research or legal purposes, these documents must be properly destroyed pursuant to Policy 2000, Management of University Records. Paper documents containing Social Security numbers should be shredded. Consult the ITSO standards for guidelines regarding the destruction of electronic records.

2.4 Incident Response

An incident or breach is the unauthorized access, use or release of SSN to external parties due to either inadvertent exposure or malicious attack. Virginia Tech takes every precaution to secure and protect university systems and data. Nevertheless, immediate steps should be taken to correct any security breach or exposure of sensitive data.

In accordance with the Virginia Tech Dealing With Data Exposures document, anyone who has reason to suspect a potential breach of established security policy, procedure or sensitive data should promptly report it to the appropriate Dean, Vice President/Vice Provost, Director, or Department Head. The University Police and the IT Security Office should be notified as appropriate. The university will not take disciplinary action against any person solely because of good faith reporting of a disclosure. Such individual making such notification will be protected from retaliation. Affected customers may also need to be notified after the department consults with the appropriate areas within the university. Examples of significant failures would include a successful hacking effort, a burglary, or impersonations leading to the defrauding of customers. More detailed information is available at https://security.vt.edu/incident/dealing_with_data_exposure.html.

Any inappropriate disclosure of SSNs for research must be immediately reported to Scholarly Integrity and Research Compliance.

3.0 Responsibilities

Below are distinct roles and responsibilities assigned for safeguarding the SSN.

3.1 Data Trustees

Data trustees are defined for the SSN policy as those Vice Presidents and Vice Provosts (VPs) who have oversight responsibilities for offices and functions that collect and/or report the SSN, and the Vice President for Information Technology & Chief Information Officer, who has oversight responsibilities for the storage of the SSN in enterprise databases.

Data trustees are responsible for:

- Submitting written request for approval to collect SSN to the Vice President for Finance for university operations or departments reporting to them in accordance with this policy.
- Approving or assigning a designated data steward to approve the release of SSN to external parties as defined in Section 2.2.2.

3.2 Data Stewards

With delegated authority from data trustees, data stewards are the primary contacts for members of the university community with regard to data in their domains. The data stewards, in the context of this policy, are the managers of the operational departments where processes require the university to collect, store, and use the SSN.

Data stewards are responsible for:

- Providing oversight over the functions or systems that collect or store SSN for compliance with this policy.
- Ensuring that the forms and documents requesting SSN within their area(s) of operation incorporate the standard disclosure statement (as included in Section 4).
- Conducting an annual review of access and collection of SSNs within their areas to ensure continued business need for collecting the information and to verify the access privileges.
- Submitting request to the data trustee and the IT Security Officer for approval to release SSN to external parties including contractors, vendors, or service providers, documenting the specific legal requirement or business need after consultation with the University Legal Counsel. SSNs may be released by the university to entities outside the university after approval for each instance by the IT Security Officer.
- Maintaining a list of approved entities to which the SSN may be released.

3.3 IT Security Office

IT Security Office is responsible for:

- Establishing standards and guidelines for handling sensitive data in electronic systems.
- Developing training materials, providing guidance and problem resolution regarding secure storage, transmission, and disposition of sensitive data in electronic systems. Providing periodic and ongoing training for data stewards with regard to electronic storage and use of SSNs.

- Review and approval of all instances of release of university SSNs to external parties.
- Spearheading the efforts to address incident response as stated in Section 2.4.

3.4 Vice President for Finance Office

The Vice President for Finance Office is responsible for**:**

- Providing timely response to the data trustees regarding their written request for the collection and use of SSN for university operations other than research. Evaluating written requests received from data trustees for collecting SSN ensuring the business need or legal requirement to collect the information and gaining reasonable assurance regarding the processes put in place to secure the SSN prior to providing a response.

- Maintaining an inventory of university entities approved by the Vice President for Finance to collect and store SSN in accordance with this policy.

3.5 Scholarly Integrity and Research Compliance

Scholarly Integrity and Research Compliance is responsible for**:**

- Providing timely response to researchers regarding their written request for the collection and use of SSN for research. Evaluating requests received for collecting SSN ensuring the documented research need or legal requirement to collect the information and gaining reasonable assurance regarding the processes put in place to secure the SSN prior to providing a response.

- Maintaining an inventory of university entities approved by Scholarly Integrity and Research Compliance to collect and store SSN in accordance with this policy.

3.5 University Departments

University departments are responsible for:

- Establishing processes and procedures within their areas utilizing SSN to comply with this policy.
- Ensuring employees within their departments are appropriately trained in university policies and procedures related to safeguarding the confidentiality of the SSN in both paper and electronic systems.
- Promptly reporting any breach of SSN information to their Deans, Vice President/Vice-Provosts, Director, or Department Head and the ITSO and implementing appropriate procedures to address the breach, as detailed in the Virginia Tech Dealing with Data Exposures document.

4.0 Approved Language

All university forms and documents that request SSNs must include a disclosure statement specifying the reason to collecting the information e.g. legal requirement or specific operational need and include language to indicate whether the request is mandatory or voluntary. The following disclosure statements are approved for use on the university forms. Should circumstances arise in which the following statements are not appropriate, the data administrators (data trustee or data steward) will work with University Legal Counsel to provide an appropriate alternative statement.

Student forms:

"Providing your Social Security number is required for the award of federal financial aid and issuance of Form 1098-T Tuition Statement. Your Social Security number is not required to complete your college applications. The university may disclose your Social Security number when required by law, or to external entities acting as the university's contractor or agent."

Employee forms:

"Virginia Tech is required by federal law to report income along with Social Security numbers (SSNs) for all employees to whom compensation is paid. Employee SSNs are maintained and used by the university for payroll, reporting, and benefits purposes and are reported to federal and state agencies in formats required by law or for benefits purposes. You will be assigned a university ID number that will be used to manage your employment records thereby protecting the confidentiality of your Social Security number. The university will not disclose an employee's SSN without the consent of the employee to anyone outside the university except as mandated by law, or to external entities acting as the university's contractor or agent, or required for benefits purposes."

General statement for student handbooks, course timetables, and related materials:

"Virginia Tech is committed to protecting the privacy of its students, employees, alumni, and other associated individuals. At times, the university will ask you for your Social Security number. Federal and state law requires the collection of your Social Security number for certain purposes such as those relating to employment, taxes, and student aid.

The university may make the request for your Social Security number at a time when it is easiest for you to provide it, even if the need is not yet mandatory. For example, the university is required by the IRS to supply the name, address, and Social Security number of every tuition-paying student. The university is also required to have a valid Social Security number before an individual can receive compensation. Thus, without your Social Security number, the university cannot grant an assistantship or provide other employment. Virginia Tech may ask for your Social Security number in anticipation of need, such as at application for admission or application for employment.

The university may disclose your Social Security number when required by law, or to external entities acting as the university's contractor or agent.

This statement was created for informational purposes only and may be amended or altered at any time."

5.0 Definitions

Data administration – Policy 7100, Administrative Data Management and Access Policy establishes uniform data management practices and responsibilities for assuring the integrity of university data and includes standards for high-risk digital data protection. It sets forth responsibilities for data trustees and data stewards, and describes the risk data classification (high risk, moderate risk, low risk).

Point of service – a physical or electronic interaction between the university and its employees, students or other individuals, during which the university provides physical, educational, informational, or electronic services to the individual.

High risk – classification of data where protection of data is required by law or regulation and the university is required to self-report to the government or provide notice to the individual if the data is inappropriately accessed.

Sensitive data – any data electronic or paper-based data, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on university interests, the conduct of university programs, or the privacy to which individuals are entitled. At Virginia Tech, this includes Social Security numbers, Credit card numbers, Debit card numbers, bank account numbers, driver's license numbers, and passport numbers.

SSN – primarily refers to the Social Security number assigned by the Social Security Administration, and also to the Individual Taxpayer Identification number assigned by the Internal Revenue Service to individuals. SSN excludes other government-issued identifiers, whether to individuals or corporate entities.

Virginia Tech ID number (VT ID number) – alphanumeric string that uniquely associates various records with an individual within the university administrative information system.

6.0 References

Virginia Government Data Collection and Dissemination Practices Act
Government Data Collection and Dissemination Practices Act (virginia.gov)

Policy 7100: Administrative Data Management and Access Policy
http://www.policies.vt.edu/7100.pdf

Standard for Administrative Data Management
https://it.vt.edu/content/dam/it_vt_edu/policies/AdministrativeDataManagementStandard.pdf

Standard for High Risk Digital Data Protection
https://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf

Division of Information Technology: Policies & Standards
https://it.vt.edu/resources/policies.html

Records Management Services Procedures
https://lib.vt.edu/find-borrow/rms.html

IT Security Office: Protecting Sensitive Data
https://security.vt.edu/resources/sensitiveinfo.html

Policy 2000: Management of University Records
http://www.policies.vt.edu/2000.pdf

Dealing with Data Exposures
https://security.vt.edu/incident/dealing_with_data_exposure.html

Code of Virginia § 2.2-3808
https://law.lis.virginia.gov/vacode/title2.2/chapter38/section2.2-3808/

Set-Off-Debt Collection Act: Code of Virginia § 58.1-521
https://law.lis.virginia.gov/vacode/title58.1/chapter3/section58.1-521/

Privacy Act of 1974 (US Code)
https://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf

7.0 Approval and Revisions

Approved May 25, 2007 by the Executive Vice President and Chief Operating Officer, James A. Hyatt.

- Revision 1
  Policy underwent a comprehensive revision to include reference to Data Security policy and standards, addition of "Responsibilities" section delineating roles and responsibilities for implementation of the policy, addition of language related to handling of incident response, and updated approved language for inclusion in forms and documents requesting SSN.

  Approved April 23, 2021 by the Senior Vice President for Operations and Chief Business Officer, Dwayne L. Pinkney.