

Social Security Number Initiative: Remediation Guidance Document for Departments

The University is undertaking a comprehensive initiative to phase out systematically its use of Social Security numbers (SSNs) wherever possible. Although SSNs must be collected for selected business functions, such as meeting Federal requirements to produce W-2 tax forms and financial aid reporting, the University will be altering other business functions to use University ID numbers in place of SSNs wherever possible.

The transition away from SSN use will take time and will likely not occur without some inconvenience and process disruption. However, the resulting enhancement in the privacy and security of personal information the University must maintain about its students, faculty, and staff makes the effort very worthwhile.

What Departments Must Do

A University policy regarding SSN protection and usage, reflected in the guidance below, has been issued <<https://etg07.itc.virginia.edu/policy/policydisplay?id=IRM-014>>.

The University of Virginia collects and maintains SSNs of students, faculty, staff, alumni, patients, applicants for admission, vendors, visitors and other constituencies in approved business processes and as required by law. The University classifies SSNs as *highly sensitive data* and will:

- handle this information with a high degree of security and confidentiality and in compliance with University policies, regulations, and laws;
- collect and store SSNs only when they are essential for approved business processes or to meet legal requirements, such as the generation of W-2 tax forms;
- inform individuals who are asked to supply SSNs whether they are legally required, or may refuse, to supply the SSN, and also of any specific consequences of providing or not providing the information.
- display SSNs on online screens, reports, and other forms of presentation, or otherwise provide copies of SSNs, only to those authorized to view this information and only when needed for an approved purpose;
- authorize the fewest number of people possible to access SSNs in both electronic and non-electronic form;
- maintain an accurate inventory of records that contain SSNs;
- dispose of electronic and non-electronic records containing SSNs in a responsible manner that minimizes the risk of unauthorized access, in accordance with the University's [Electronic Data Removal Policy](#) and [Records Retention and Disposition Policy](#), e.g. shred paper records on which SSNs are printed;

The University will NOT:

- print SSNs on identification cards or badges or include SSNs in magnetic strips or bar

- codes;
- use SSNs as the account numbers or identifiers for individuals in new electronic or non-electronic records or record systems unless needed for an approved purpose or required by law.

In order to meet the policy requirements, departments will need to get approval before using SSNs in any new way. By July 1, 2008, departments will need to identify all records and records systems within their purview that use SSNs and develop a remediation plan, which, following approval, must be implemented by July 1, 2009.

Materials available at U.Va.'s SSN Initiative web site <<http://www.virginia.edu/ssninitiative>> include a [form for requesting approval for new SSN use](#) and a [template for the report due July 2008](#). Completed documents should be sent via messenger mail to: SSN Initiative Project Management Team, c/o Brian Davis, VP/CIO's Office, Box 400217.

How To Get Started: (IRS)²

1. Identify and Inventory

Establish a team leader for this project within your department and work to inform and educate department members about the need to review and likely change processes.

Review each of your departmental information systems – both computing- and paper-based – identifying where you

- solicit or collect SSNs
- store SSNs
- use SSN as an account number or identifier
- use SSNs in interactions with other systems at the University
- share SSNs with third parties outside the University
- have archived or other “old” records that include SSNs
- display SSNs on any documents or screens
- include SSNs on any mailed documents
- transmit SSNs over the Internet or through other data connections (including fax)
- send SSNs in e-mail
- store items with SSNs in a document imaging system

An “[Identify and Inventory](#)” document, including a list of questions to ask (with examples of systems and processes to be considered) and a tracking template, are included in the report template referenced above.

This review can be enhanced by the use of software designed to scan computers for SSNs and other types of sensitive data. This can be particularly useful to confirm that individual workstations and laptops are clear of unmanaged sensitive data. UVa has purchased a bulk

license to provide copies of such software called Identity Finder for all faculty and staff <<http://www.itc.virginia.edu/security/identityfinder/>>. Another such product that ITC has made available is Spider, a free, open source product created at Cornell University <<http://www.itc.virginia.edu/security/spider/>>.

2. Remediate and Reduce

For each of the processes or systems identified in step 1, the department must develop a plan either to

- remediate the process or system by completing removing SSN usage, or
- reduce SSN usage to the absolute minimum but retaining it as necessary for a legal requirement or approved business use.

Understand that the goal of the policy is to eliminate use wherever possible, and that approval to retain SSNs will be intentionally limited. Such a plan should also prioritize among affected systems and identify any dependencies between affected systems. A [template for this plan](#) is included in the report template referenced above. This plan should be submitted as described above by July 1, 2008. Earlier completion dates will be necessary for centrally maintained systems that prevent schools, departments, divisions, and business units from moving forward with their remediation plans.

Even if there is a [legal requirement or approved business use](#) requiring retention of SSNs, you are required to reduce that use as much as possible:

- restrict access to SSNs to the absolute minimum number of individuals
 - includes data entry, data viewing, report viewing and physical access
 - inventory personnel with access to SSNs along with their access level
 - provide continuing education regarding proper handling of sensitive data to users of SSNs
- even if the system requires SSNs internally, remove them from all screens, reports and print outs where they are unneeded, or use only the last 4 digits of the SSN where sufficient
- delete any historical data containing SSNs that are no longer needed or do not need to be retained by legal requirement; examples include
 - gradebooks
 - spreadsheets
 - data downloaded from ISIS or the Information Warehouse to produce reports (you can re-download the data later if needed)

3. Secure and Sustain

Any retained SSNs are classified as highly sensitive data, and are subject to the “Data Protection Standards for Highly Sensitive Data” (forthcoming, early 2008). These standards will require **very strong security measures** to protect all computers and filing cabinets storing SSNs and to protect all SSN data in transmissions, as well as two-factor

authentication for access, a customized hardware firewall and an annual departmental risk assessment. Departments are also required to sustain the process by continually reviewing all uses of SSN, seeking new opportunities to remediate or reduce, and improving security measures as needed.

Implementation of the approved plan for remediation, reduction and securing of SSN must be completed by July 1, 2009.

Contacts

The SSN Initiative web site with additional information is at <http://www.virginia.edu/ssninitiative>. Contact ssn-initiative@virginia.edu with any questions.

Version Notes

The only difference between 1.0 (12/07) and 1.1 (02/08) is the removal of the FAQs, which are posted separately at <<http://www.virginia.edu/ssninitiative/faqs.html>>, where they are updated regularly.

Version 1.2 (04/08) added reference to Identity Finder software.