

Individual SSN Attestation Form
Removal from Usage or Protection of SSNs (Social Security Numbers) After September 30, 2006

The University policy is to cease using Social Security Numbers (SSNs) in electronic files and on computer systems effective September 30, 2006. After that date, unencrypted SSNs are to be stored only on highly secured central systems, or on systems for which exceptions have been applied for (via the SSN Exception Form available at <http://csuid.colostate.edu/?page=forms>) and granted. By September 30, 2006, CSU employees are to complete and return this form to their department or unit head for forwarding to ACNS. If item 2 below is checked, individuals should 1) work with their IT support staff to scan their computers and their file systems for SSNs, as they individually judge appropriate, and 2) apply for exceptions for files and electronic systems where use of SSNs needs to continue. Please refer to the guidelines below for additional information about performing this exercise.

If you have any questions concerning this matter, please visit <http://csuid.colostate.edu>, or contact Patrick J. Burns, Patrick.Burns@colostate.edu, 491-5778. Thank you for your efforts in this regard.

I hereby certify that (check one of the two options below):

1. In my job at CSU, I do not access SSNs via electronic systems, nor do I possess SSNs in other form (e.g. paper); OR
2. I certify that:
 - a. I understand that I am responsible for securing access to personal information under my control, including Social Security Numbers (SSNs).
 - b. To the best of my knowledge, SSNs in significant quantity have been removed from my electronic files and computer systems, and the appearance of SSNs in my files is at most incidental (e.g. they are embedded in small numbers deep within files and not readily accessible in significant numbers), or SSNs in significant quantity have been protected via encryption. This includes all electronic files that are under my control (e.g. spreadsheets, databases, locally stored email, word processing documents, reports, and/or any other type of electronic file, and files stored on shares), on all types of computers (servers, desktops, laptops, PDAs, mobile communication devices/cell phones, etc.) including personal and home computer systems that I use for University business, and media of all formats (hard disks, floppy disks, removable disks, memory sticks, memory cards, etc.). It does not include files on servers that are not under my control (e.g. central files that I do not own – work with your IT support staff if you have questions about this). For additional detail, see the Guidelines for Compliance to SSN Sweep below.
 - c. I have applied for exceptions where appropriate (the SSN Exception Form is available at <http://csuid.colostate.edu/?page=forms>).
 - d. All hardcopy forms and electronic forms under my control have been modified so as no longer to request SSN. And
 - e. I have physically secured (e.g. behind locked doors, or in locked file cabinets) hardcopy forms, documents and other media containing SSNs.

Attestation signed by individual:

Department Name: _____ Dept. Number: _____

Printed name

Signature

Date

Guidelines for Compliance with SSN “Sweep”

This document provides guidelines for complying with the University requirement to remove and/or protect Social Security Numbers (SSNs) from individuals’ files and computer systems. The guidelines are just that – guidelines. No prescriptive formula or checklist can be given, as this would remove the capability to exercise judgment individually, and this is not the intent of this exercise.

The following steps are suggested in order to minimize and mitigate your risk associated with SSNs on University systems.

1. Rather than deleting files containing SSNs, you may choose to encrypt and therefore protect SSNs on your file systems. One option for doing so is to use the University-approved freeware Truecrypt. Alternatively or additionally, you may wish to use encryption built into your operating systems. Please coordinate encryption measures with your local IT support staff.
2. Write files containing SSNs that you must retain onto physical media (CDs, DVDs, etc.), and secure that media as you would any non-electronic document or file containing sensitive information, e.g. behind locked doors, in locked file cabinets, etc. Do not leave the media in your computer and therefore accessible, but keep it locked up elsewhere unless and until you need it. Remember to delete the files on your systems after you have written them to CD, DVD, etc.
3. Remove SSNs from your files:
 - a. Delete all old, unused files containing SSNs. Try to access SSNs only on central systems, rather than downloading them to your local systems or to shared storage space.
 - b. Open up all old grade files (e.g. in Excel), and delete the columns containing SSNs/PIDs. Make sure you are not deleting information in that column that you may wish to keep. Make sure you do this also in old back-up files.
 - c. Do the same for all other files containing significant quantities of SSNs.
4. After you have removed SSNs from your systems and files to the best of your ability, and consistent with these guidelines, work with your IT support staff to have your file systems scanned for SSNs using the University approved scanning tools – see <http://csuid.colostate.edu>. Please include your personal computers, your files on servers (shares), your files on back-up devices, etc. in your scans. If you believe that you have SSNs in files on portable devices, e.g. USB memory sticks, etc., please consider having these scanned for SSNs as well.
5. You are not expected to remove SSNs that appear incidentally deep within your files and file systems. Specifically, it is not expected that you remove files or SSNs in files where only a few SSNs are embedded (for example, in large, old email archives), where it would be difficult for someone to wade through the information to access SSNs if they had access to those files.
6. SSNs located on paper documents and in files stored on physical media have been secured, for example behind locked doors, or in locked file cabinets.