

TEXAS A&M UNIVERSITY-CORPUS CHRISTI
Individual Social Security Number Attestation Form

Social Security Number Removal or Protection

Check one of the two options and sign below.

I hereby certify that:

1. In my job at Texas A&M University-Corpus Christi, I do not access Social Security Numbers via electronic systems, nor do I possess Social Security Numbers in any other form (e.g. paper) and I have verified that Social Security Numbers do not exist on any information resource I have been assigned.

OR

2. I certify that:
- (1) I understand that I am individually responsible and accountable for securing access to sensitive information under my control, including Social Security Numbers.
 - (2) To the best of my knowledge, Social Security Numbers on systems and devices under my control have been protected via encryption when not being specifically accessed. 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, mobile computing devices, etc.), including personal and home computer systems that I use for university business, and media of all formats (hard disks, floppy disks, CD/DVD-ROMs, 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 details, see the Guidelines for Compliance with Social Security Numbers Removal or Protection below.
 - (3) Enrollment Management (Social Security Numbers for students) or Human Resources (Social Security Numbers for faculty/staff) has been notified, via the Social Security Number Storage Exemption Form, and approved storage and use of Social Security Numbers for each information resource and storage location that I have been assigned responsibility.
 - (4) Enrollment Management (Social Security Numbers for students) or Human Resources (Social Security Numbers for faculty/staff) has approved all hard copy forms and electronic forms under my control that request Social Security Numbers.
 - (5) I have physically secured hardcopy forms, documents, and other media

TEXAS A&M UNIVERSITY-CORPUS CHRISTI
Individual Social Security Number Attestation Form

containing Social Security Numbers, when not in use, and maintain a list of authorized personnel who may access the storage device and the area where the storage device is maintained.

- (6) I understand that any information resource containing sensitive information, including Social Security Numbers, must be listed as a Critical resource when completing the annual ISAAC risk assessment reports associated with that information resource.

Attestation signed by individual:

Department:

Individual's Printed Name:

Individual's Signed Name:

Date Signed:

TEXAS A&M UNIVERSITY-CORPUS CHRISTI
Individual Social Security Number Attestation Form

Guidelines for Compliance with Social Security Number Removal or Protection

This document provides guidelines for complying with the Texas A&M University-Corpus Christi requirement to remove and/or protect Social Security Numbers 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 document.

The following steps are to be utilized to minimize and mitigate the risks associated with Social Security Numbers on university and personal computers, mobile computing devices, and storage devices.

1. Work with your information technology support staff to have your file systems scanned for Social Security Numbers using the university approved scanning tools. Guidance for scanning systems can be located on the Texas A&M University-Corpus Christi Information Technology Security web page located at <http://security.tamucc.edu>. Include all university and personal computers, mobile computing devices, and storage devices that have or may have been utilized for work related to this university.
2. Files containing Social Security Numbers must be encrypted when not being directly accessed. These files should remain encrypted even after an individual has logged into the information resource until the information within the file itself is specifically going to be utilized. There are several encryption options available depending on the operating system running on the information resource being used to access the information. Encryption methods should be coordinated with your department information technology support staff. Recommendations can be found on the Texas A&M University-Corpus Christi Information Technology Security web page located at <http://security.tamucc.edu>.
3. Files containing Social Security Numbers that must be maintained but are not necessary for immediate access can be removed from systems by encrypting and writing the files onto physical media (CDs, DVDs, etc.). Media containing Social Security Numbers must be secured as you would any non-electronic document or file containing sensitive information, e.g. behind locked doors, in locked file cabinets, etc. Remember to securely delete the unnecessary files on your systems after you have written them to CD, DVD, etc.
4. Where appropriate and after verifying the information is not necessary, completely remove files containing Social Security Numbers: Electronic files should be securely deleted utilizing a secure deletion or wiping utility. Hard copy files should be destroyed using a cross-cut shredder. If a file must be maintained but Social Security Numbers are deleted from the information contained in the file (e.g. deleting a column from a Microsoft Excel spreadsheet) a method for

TEXAS A&M UNIVERSITY-CORPUS CHRISTI
Individual Social Security Number Attestation Form

removing hidden data must be used. Removing hidden data will ensure that the Social Security Numbers cannot be restored in future versions of the document.

5. You are not expected to remove Social Security Numbers that appear incidentally deep within your files and file systems. Specifically, it is not expected that you remove files or Social Security Numbers in files where only a few Social Security Numbers are embedded (for example, in large, old email archives), where it would be difficult for someone to wade through the information to access Social Security Numbers if they had access to those files.
6. Individuals who access Social Security Numbers on printed documents or forms on a regular basis should consider adhering to a clean desk policy. A clean desk policy means that no document is left exposed unless an authorized individual is within the immediate vicinity of the desk in question and can control physical access to any document located on that desk.
7. Filing cabinets containing sensitive information must be locked when authorized personnel are not in the immediate vicinity and can control physical access to the cabinet. These filing cabinets should be maintained in an area that can only be accessed by authorized personnel.