

## ***DON'T COMPROMISE!***

### **Best Practices for Protecting Social Security Numbers @ the University of South Carolina**

---



The University of South Carolina collects and maintains Social Security Numbers (SSN) of employees, students, and others associated with the University as required by law. It is the policy of the University to protect the privacy of Social Security Numbers.

USC is dedicated to ending the use of the SSN as a key identifier, and this process will begin in the academic year 2006-07 with the implementation of a new integrated student and administrative information system. However, USC will need to maintain the 9-digit SSN as the key identifier in student, business, and human resource systems until the conversion to the new system has been completed.

It is **essential** that all faculty, staff, and students who require the use of SSNs adhere to the following practices:

- ☒ NEVER store SSNs on computers that are not secure.
  - NOTE: *Just because a system requires a password does not mean it is secure.* Servers may be open to the Internet and subject to search engine harvesting/caching. Ask your network manager or go to <http://security.sc.edu> for more information.
- ☒ DO NOT send social security numbers via e-mail.
- ☒ NEVER ask a person to speak his/her SSN in a public setting.
  - Ask him/her to write it on scrap paper. Shred the paper after reading it or return to student.
  - Ask him/her to key it into a numeric auxiliary keypad for digital input.
  - Swipe his/her CarolinaCard.
  - When acquiring the SSN by telephone, ask ... “Are you in a private location where you can give me your SSN verbally?”
- ☒ REMOVE the SSN from reports and screens where it is not required. When printed, protect the SSN from being seen by others.
- ☒ SHIELD monitors when SSNs are displayed because they should not be accessible to others. Use a monitor visor or hood in service areas.
- ☒ DESIGN web applications that mask the SSN like a password.
- ☒ SHRED all documents that contain SSNs and other confidential material, as appropriate, to dispose of it in a manner that prevents its exposure.

Even after the implementation of the new system, the SSN will be maintained as a data element in University systems for purposes of employment, IRS reporting, and financial aid. SSN protection must always be a fundamental practice.

Knowledgeable staff members from several University offices are available to answer questions you may have or provide advice. They may be reached by e-mail at [privacyconcerns@sc.edu](mailto:privacyconcerns@sc.edu) or by telephone at 777-3541.