IT Security Office
Version 2.3 02/19/10

Mitigating Protected Level 1 Information Storage

San Diego State University is required to inventory and report the storage of protected level 1 information annually. In order to meet this requirement several tools are provided for users/departments/auxiliaries to use to locate the information, reconcile and report the secure storage of the information.

Identifying Social Security and credit card numbers is complicated and the search tool report may contain false positives. Each user should review the report to validate the information. If the information is valid, the user must then chose the most secure option from the instructions below to remediate the risk of storing protected level 1 information. The instructions are listed in the order of most secured to least secured.

1. Delete the file. If user no longer needs the file containing the SSN/credit card information, delete it.
2. Delete the SSN information. The user can delete just the SSN/credit card information (if not needed) and still leave the remainder of the form/letter in tact.
3. Archive the file. If the information is needed for reference, but not needed on-line, print it, burn a CD-R/DVD, or save the file to a tape, and remove the information from the system. Be sure and store the print out/storage media now containing the SSN information in a secure area.
4. Move the file to a protected file server. Contact IT support staff for directions to the best file storage for your department/college.
5. If the information is stored in temporary browser files this would occur if a user opened a file containing SSNs with their browser. If these files do contain SSNs then the user needs to minimize storage of this information on the system. IT support staff can set the user's browser so that temporary internet files are deleted after the user closes their browser. IT support staff should test this setting on one user and see the affects before applying to all users.
6. Users should not email SSN information. If emails are being sent in order to share information, please see step 3 for setting up a secure area on a file server. Let IT support staff know if there is another reason for using email and they will assist with an alternate solution or invite the IT Security Office to assist.
7. If the information is stored in the desktop trash, work with IT support staff for automated controls to empty the trash when the system shuts down or reboots. If automated controls are not possible, the user will need to manually empty the trash at least weekly.
8. Some findings indicate that old information, possibly unrelated to the current user and their job, might be stored on the system. If so, please contact the appropriate manager of the information and schedule a transfer of the information or destruction. All systems should be rebuilt before being assigned to a new user. Work with IT support staff to ensure this is done properly.

We must do all we can to remove or limit the storage of SSN and credit card information on networked systems as this poses the highest risk to the information.