Protected Information process checklist (section 3.1.1 & 3.1.3)
Information Security #8

March 31, 2011

The left column indicates whether the standard is listed in the Information Security Plan as a **M**ust or **S**hould. A justification must be written for any standard not followed in the department procedures. The justification must be approved by the IT Manager for items listed as a **S**hould and also reviewed with the IT Security Office if the item was listed as a **M**ust. The IT manager must review, sign and date, all exceptions every six months to indicate that the exception is still necessary.

Protected Level 1 data consists of:

a. Account passwords or credentials.
b. PINs (Personal Identification Numbers).
c. Private key (digital certificate).
d. Name with credit card number.
e. Name with Tax ID.
f. Name with driver's license number, state identification card, and other forms of national or international identification.
g. Name with birth date combined with last four digits of SSN.
h. Medical records related to an individual (including disability information).
i. Psychological counseling records related to an individual.
j. Name with bank account or debit card information with any required security code, access code, or password that would permit access to an individual's financial account.
k. Name with personally identifiable information:
   - Mother's maiden name.
   - Employee net salary.
   - Employment history (including recruiting information).
   - Biometric information.
   - Electronic or digitized signatures.
   - Names of parents or other family member.
   - Birthplace (city, state, country).
   - Race and ethnicity.
   - Gender.
   - Marital status.
   - Personal characteristics.
   - Physical description.

M/S	Item	Y/N
M	1. Departments must participate in the Protected Level 1 Authorization Access Approval reporting process described in section 3.1.2 every semester. The Information Security Office must have a copy of the authorized access, justification, and location on file.	
M	2. All employees with access to PL1 data must complete the CSU Security Awareness online training. Contact iso@sdsu.edu to request enrollment.	
M	3. Review table 3-1 (see BELOW) and document department handling of PL1 information.	

Protected Information process checklist (section 3.1.1 & 3.1.3)
Information Security #8
March 31, 2011

M/S	Item	Y/N
S	4. Deploy Find_SSN to every storage system (desktops, laptops, web and file servers) to locate Social Security numbers. Document the process used to run the program, the aggregate information found, and mitigation strategies used. Links to Find_SSN program on next page.	

Process/storage/use	Secure handling of PL1 data Note: Table 3-1 in ISP details handling of PL2 data
Transmitted via fax	Must be attended at both ends until completion With approved procedures **A**
Transmitted outside of SDSU network (includes remote access)	Must be encrypted With approved procedures
Transmitted in internal SDSU network **B**	Must be encrypted With approved procedures
Included in e-mail content **C**	Must be encrypted With approved procedures
Permanently stored on desktop computer (should be accessed via secure file server)	With approved procedures
Stored on personally owned equipment or at personal home	No **D**
Stored in database	Should be encrypted **E** With approved procedures
Stored on mobile device	Must be encrypted With approved procedures
Stored on server	Should be encrypted With approved procedures
Left unattended in work area	With approved procedures Physically secured if accessible by unauthorized individuals
Paper disposal	Shred immediately Physically secured until shredded With approved procedures
Electronic media disposal	Electronically overwritten or destroyed Secured until disposed With approved procedures
Document, container, and media labeling **F**	Should be labeled "Protected Level 1" Should be physically secure
Left on voice message	Must have password-protected voice messaging With approved procedures
Discussed verbally **G**	In private area
Sent through campus mail **H**	In sealed container Not visible outside container Tagged "Confidential"
Sent through postal/ common carrier mail	In sealed container Not visible outside container Tagged "Confidential"

A Except for credit card information for payments to the University, which may not be faxed without Controller authorization.
B May be technically infeasible for SQLNet, printers, some file sharing, fax, and copiers.
C Received e-mail attachments, even encrypted, must be saved to a secure location and deleted from e-mail.
D Cell phones used for authorized University purposes may store, with approval, and must be encrypted.
E The name of the individual does not have to be encrypted.

Protected Information process checklist (section 3.1.1 & 3.1.3)
Information Security #8
March 31, 2011

F As supported by the application. Documents include forms. Stamps/stickers with "Confidential" labeling are acceptable. Term "container" does not refer to laptops or mobile devices.
G In accordance with federal, state, and local laws. Does not refer to e-mail.
H When possible, best to hand-deliver protected level 1 and 2 information.

Links to Find_SSN program:
http://www-rohan.sdsu.edu/~findssns/run_xp/Running_Find_SSNs_on_Windows_2000_and_XP.html
http://www-rohan.sdsu.edu/~findssns/run_vista/Find_SSNs_Vista.html
http://www-rohan.sdsu.edu/~findssns/run_mac/Running_Find_SSNs_on_Mac_OS_X.html
http://www-rohan.sdsu.edu/~findssns/review/Reviewing_the_Results_of_the_Find_SSNs_Program.html