Information Security #3 checklist (section 3.9.7)

Excludes 3.9.7.1

October 5, 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.

M/S	Item	Y/N
M	1. IT Managers much ensure a backup plan is developed and implemented by IT support staff. It must address these scenarios:	
M	a. Recovery of files accidentally deleted (single file).	
M	b. Hardware failure (recovery of software/data on a drive).	
M	c. Incident response investigation (recovery of uncompromised software/data).	
M	d. Disaster recovery (complete rebuild of server).	
S	2. Items to include in backup plan are:	
S	a. Schedule for the backups.	
S	b. Encryption of PL1&2 data.	
S	c. Daily check of backup logs (i.e. did backup complete normally).	
S	d. Verification of information backed up (i.e. were all items backed up).	
S	e. Testing restores (can the data be recovered)?	
S	f. Type of backup (full, incremental, differential) depending on rate of changes and speed of backup recovery resources.	
S	3. It manager should work with IT support staff to determine best backup strategy or combination of strategies to restore information in a timely manner.	
S	4. Reference: http://security.sdsu.edu/iso/pdfs/Backup_Strategies.pdf.	