# Information Security #4 checklist (section 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 |
|---|---|---|
| S | 1. Multiple backup media should be used in the process (i.e. different media for each daily, monthly, yearly). | |
| S | 2. For recent backups (daily, weekly) that may need quick retrieval, store media in fireproof safe or locked storage container in an alternate building. | |
| S | 3. Longer term backups (monthly, yearly, archive) store media offsite (contact UCO Director to see about joining data center contract) | |
| S | a. Offsite vendor specializes in information storage. | |
| S | b. A contractual agreement established with the vendor. | |
| S | c. List of authorized IT staff for requesting tapes. | |
| S | d. 7/24 SDSU staff access to media. | |
| S | e. Chain of custody for media (i.e. logging and tracking pickup/delivery/inventory). | |
| S | 4. Two backups for critical information. | |
| S | 5. IT support staff notify manager immediately if backups fail. | |
| S | 6. Retention and refresh schedule for media (tapes wear out). | |
| S | 7. Failed media sent to Material Management for shredding. | |
| S | 8. IT Manager ensure backup restores are scheduled to ensure media is viable | |
| S | a. Scripts can be used to automate test restore process of a few files. | |
| S | b. Beginning, middle, and end of media tested. | |