Storing, distributing, & encrypting protected information checklist (section 3.9) Information Security #2

December 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. Protected level 1 information should be stored on secured databases or file servers or off-line media (such as CD and DVD storage).	
S	2. Off-line media should be encrypted.	
S	3. Off-line media should be stored in a secure location.	
M	4. When using campus mail or an outside carrier to send protected level 1 or 2 information, the protected information must be sealed, invisible from the outside, and marked “Confidential”.	
M	5. When leaving voice messages of send protected level 1 or 2 information, the messaging system must be password protected.	
M	6. When faxing protected level 1 information, the fax machine must be attended.	
M	7. Protected level 1 information must not be stored on personal equipment (such as laptops, desktops, PDAs, iPod, cellphones, etc.).	
M	8. Protected level 1 information must not be forwarded to personal email accounts.	
M	9. IT Managers are responsible for ensuring access to information on file servers is limited to authorized users.	
S	10. Protected information stored on file servers should be encrypted.	
M	11. IT Managers are responsible for ensuring access to protected information in databases is approved according to job duties via read/write privileges on database objects.	
S	12. Databases should be configured to encrypt protected level 1 elements.	