Desktop Laptop Mobile Device #5 checklist (section 3.2.4)

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. Authorized software:	
M	a. Has to be approved by the IT manager.	
M	b. It must perform functions that support the department's mission and the needs of the University.	
M	c. It must be legally licensed for the department's use.	
M	2. IT manager assess the potential risks/benefits of software before approving.	
S	3. Peer-to-peer file sharing, personal, and non-University related software should not be approved.	
M	4. IT support staff must not take actions contrary to the license agreement:	
M	a. Make copies for use on desktops for which it has not been purchased.	
M	b. Put copies on the network unless restricted to authenticated and authorized access.	
M	c. Obtain copies from others without paying the appropriate licensing fee.	
S	5. IT support staff utilize system security to prevent users from loading/executing unauthorized software on desktop.	
S	6. IT support staff should inspect/test new/custom software to:	
S	a. Determine compatibility with existing authorized software.	
S	b. Discover/disable any utilities used to compromise the OS or logical access.	
S	c. Identify unforeseen interactions, such as starting a new insecure service.	
M	7. IT manager ensure configuration management procedures for authorized software are followed.	