Desktop Laptop Mobile Device #4 checklist (section 3.2.3 & 3.4.1)

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. IT managers should ensure standard hardware and software configurations are applied throughout the department.	
S	2. IT support staff build new systems in isolated network/off network until all security patches and configurations applied.	
S	3. Typical standard build contains:	
S	a. Sanitize the hard drive.	
S	b. Load and configure the appropriate operating system modules.	
S	c. Turn off unwanted services.	
S	d. Schedule and load the appropriate service packs and patches.	
S	e. Schedule and update drivers.	
S	f. Configure the network settings.	
S	g. Configure other hardware settings (video, sound, and so on).	
S	h. Test required operating system functionality.	
S	i. Schedule, load, and update anti-virus and anti-spyware software.	
S	j. Schedule, load, and update patch management and inventory software.	
S	k. Configure security on screen savers and power options.	
S	l. Rename and set passwords for appropriate system accounts.	
S	m. Load and configure the appropriate application software.	
S	n. Test all required application software functionality.	
S	4. For Windows systems, disable AutoRun function.	
M	5. IT manager meet periodically with IT to approve standard OS/software changes.	
M	6. Add desktop/laptop to inventory (computer name, OS, IP/DHCP, MAC, equipment tag, serial number).	