Server Security #3 checklist (section 3.2.2 & 3.4.4)

November 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. Anti-spyware (AS) active on all systems that open email, browse the Internet, or store data files. Settings:	
S	a. Daily AS scans	
S	b. Check for updates twice a day	
S	c. Daily reporting	
S	d. Review spyware since last report found on scan	
M	e. Report spyware found on scan (except cookies, adware, & attachment directory)	
S	f. Active protection enabled	
S	2. Email servers scan email for spyware before delivering mail	
S	3. Centralized log management of clients installed, AS updates, scheduled scans completed, scan results	
S	4. Enter rule for new spyware signature as needed	
S	5. Document any scanning area exceptions	