

Anti-virus process checklist (section 3.2.1 & 3.2.2)

DT/LT/Mobile Device Security #2 & #3

March 2, 2011

The left column indicates whether the standard is listed in the Information Security Plan as a **Must** or **Should**. 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 **Should** and also reviewed with the IT Security Office if the item was listed as a **Must**. 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. Run on all systems with email, browse the Internet, or shared files	
S	2. Centralized log management	
S	3. Active protection enabled	
S	4. Daily scans	
S	5. Clients check for updates twice a day	
S	6. Server check for updates once an hour	
S	7. Daily reporting	
	❖ Infections since last report found on scan	
	❖ Update errors	
	❖ Scans completed normally	
	❖ Current signature files (follow up within 5 weeks for desktops)	
S	8. Enter rule for new signature	
S	9. Explain any scanning area exceptions (okay for system but not IE)	