Anti-virus / Anti-spyware Interim Support Practices

(March 25, 2010)

This document defines the interim support practices required to actively manage the system ePO anti-virus/anti-spyware environment it is functioning correctly. These practices will be incorporated into the malware standards in the near future.

Active management of the environment requires the following activities are completed on an on-going basis by the colleges and the system data center (SDC).

1. Management of the McAfee Management Server (ePO) – SDC
    - Manage server environment
    - Upgrade server software
    - Upgrade McAfee ePO software
    - Develop operational standards for anti-virus and anti-spyware
    - Develop and manage operational procedures for anti-virus and anti-spyware
    - Develop standard reports to support operational procedures
    - Monthly / quarterly operational reports
2. McAfee anti-virus / anti-spyware operations – Colleges and SDC
    - Verify computers are in compliance with operational standards
    - Analyze malware detections to determine investigation requirements
    - Correct any computer not in compliance with operational standards
    - Take out of service any system requiring forensic investigations
3. Operational review and assurance – system office
    - Weekly / monthly verification of operational procedures at the colleges and SDC
    - Assurance review of security program for anti-virus & anti-spyware
4. Education / Training / Knowledge Transfer – SDC
    - Training on McAfee products and enterprise standards & procedures
    - Training development and delivery

Implementation/Support Structure

The implementation structure uses the working group concept of college and SDC developing an operational framework. The working group will provide support to the college for implementation and on-going support. Support will be structured based on the following:

- The management server will be located at the SDC and managed by the SDC staff (see Item #1 above)
- The Malware Working Group (MWG) will develop operational standards and procedures.
- The MWG will work with each college to transition their systems to the enterprise environment and train their IT staff on the associated standards and procedures.
- Each college and the system office will be responsible for managing anti-virus and anti-spyware (see Item #2 above)
- The SDC will be responsible for incident investigation when a system is potentially infected
- Both the SDC and College IT will have visibility to the management environment
- The Information Security Program Office will be responsible for verifying the colleges and system office are following operational procedures

Support Requirements:

- Operational activities occur daily (see Item #2 above)
- Colleges will need three (at a minimum two) staff trained and actively managing (e.g. rotational basis) the daily operational activities.
- SDC will need at least three (at a minimum two) staff to actively manage the anti-virus and anti-spyware enterprise functions (see Items #1, 3, 4 above).
- Notifications of possible virus/spyware infections need to be reviewed within 2 business hours
- Any storage device requiring forensics needs to be delivered to the SDC with 48 business hours
- ISPO will produce operational management reports at a minimum quarterly after the implementation is complete

Operational Procedures

A comprehensive set of operational procedures for administration, installation and operations have been developed for the management of anti-virus and anti-spyware. The procedures are located at https://www.commnet.edu/it/security/ITTechAccess/ePO/ePOProcedures.asp

Note: the website requires NetID authentication. If you are having trouble accessing the procedure please contact the Information Security Program Office at security@commnet.edu.

Anti-virus / Anti-spyware Interim Support Practices

(March 25, 2010)

Staffing:

The following are the estimated staffing requirements to manage the anti-virus and anti-spyware environment. These estimates are based on the malware working group experience with managing anti-virus and anti-spyware. The staffing assumes the project phase of transitioning to the new environment is complete and represents only the operational staff requirements. The staffing requirements are expressed as a percentage of the staff time required to perform the operational tasks.

Major Activities	SDC	Colleges		
		Sm	Med	Lrg
1. Management of the McAfee management server (ePO)	0.2			
2. McAfee anti-virus / anti-spyware operations	0.2	0.2	0.4	0.6
3. McAfee anti-virus / anti-spyware operational compliance	0.1	0.1	0.1	0.1
3. Operational review and assurance	0.2			
4. Education, training and knowledge transfer	0.1	0.1	0.1	0.1
Total staff by SDC and college size	**0.8**	**0.4**	**0.6**	**0.8**
Total staff by SDC and college	**0.8**	**7.2**		
Total staff	**8**			

Small (Sm): Less than 150 staff and faculty systems
Medium (Med): Between 150 and 300 staff and faculty systems
Large (Lrg): Greater than 300 staff and faculty systems