MCAFEE ANTIVIRUS SOLUTION COMPLIANCE

1. Purpose

The purpose of this standard is to establish the requirements and responsibilities of McAfee antivirus solution compliance for institutionally owned laptop computers. This standard provides the definition of compliance with the McAfee antivirus solution and supersedes McAfee's definition of compliance within ePO.

2. Definition

2.1. McAfee Antivirus Solution. The current UNT System IT Shared Services sanctioned McAfee software that detects computer viruses and mitigates the threats posed by computer viruses and other types of malware.

2.2. Compliance. Meeting all requirements stated within this standard.

2.3. ePO. The current UNT System IT Shared Services sanctioned end-point security management software.

2.4. IT Manager. Individual(s) delegated responsible for information technology support for a department.

2.5. Custodial Department. Department within the System Administration or Institutions that retains possession and responsibility for the laptop computer as an institutionally owned asset.

3. Scope

This standard applies to all laptop computers purchased by the System Administration and its Institutions.

4. Requirements

4.1 Laptop computers owned by the System Administration and its Institutions must meet the following requirements:

4.1.1. Must have the current McAfee Agent installed;

4.1.2. Must communicate with the ePO server every 120 days;

4.1.3. Must have antivirus definitions installed that are no more than seven days older than the last check in date; and

4.1.4. Must run supported versions of the McAfee software, the ePO agent, and the antivirus engine.

5. Responsibilities

5.1. IT Manager(s) are responsible for providing the following support to laptop computers:

5.1.1. Installing current versions of antivirus and encryption software on all newly acquired laptops prior to deployment;

5.1.2. Ensuring laptop computers receive updates and patches;

5.1.3. Investigating laptop computers that do not meet the standards established in 4.1. of this standard and documenting any variances from compliance;

5.1.4. Resolving variances from compliance that fall within their support responsibilities; and

5.1.5. Removing laptop computers from ePO when decommissioned or no longer in use.

6. Exceptions

6.1. If variances to compliance cannot be resolved, the custodial department must submit a request for a security exception. Security exception requests must be submitted to the UNT System Office of Chief Information Security Officer and include the following:

6.1.1. The custodial department name, location, and contact.

6.1.2. The service and asset tag numbers of the laptop computer.

6.1.3. Location of the laptop computer.

6.1.4. Current use of the laptop computer.

6.1.5. Reason why the variance cannot be resolved.

6.1.6. Reason why the laptop computer cannot be decommissioned.

6.1.7. Compensating controls that may mitigate the risk of non-compliance.

6.1.8. Supplemental documentation that may exist in support of the request.

6.1.9. The UNT System Office of the Chief Information Security Officer will provide an approval or rejection of the request to the custodial department.

6.1.10. The UNT System Office of the Chief Information Security Officer may revoke security exceptions at any time.

7. References

7.1. UNT System Information Security Regulation 6.1000.
7.2. UNT System Information Security Handbook.

Appendix A – Document Version Log

Version	Approved By	Date	Description
1	Charlotte Russell	2/27/2017	New Information Technology Standard
2	Rama Dhuwaraha	3/1/2017	Information Technology Mandate