**Quitman County School District**

**Technology Department**

**Anti-Virus /End Point Security Guidelines and Procedures**

**GUIDELINES**

**Introduction**

This Guideline defines the anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example, it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

**Purpose**

This guideline is designed to protect the organizational resources against intrusion by viruses and other malware.

**Detailed Guideline Statement**

Quitman County School District will make every attempt to use a single product for end point security. The following minimum requirements shall remain in force.

District Computers

•  The anti-virus software shall be installed on every computer before it is authorized to function on the district network

•  The anti-virus product will operate in real time on all servers and client computers, pending exlusions.

•  The anti-virus library definitions will be updated at least once per day.

•  Weekly scans will be setup on all Computer Devices

•  Detected threats are immediately quarantined then removed during the weekly scan.

•  Software updates are applied globally as they become available.

Non District Computers

* Non district computers are not allowed on the District’s Network. If users are granted access to the District Network via Remote access, they are required to have a current and up-to-date antivirus program installed and running in real time before a connection to the district network is granted.

**Applicability**

This guideline applies to all ipads, MacBooks, iMacs, Pcs, Laptops, and Servers that connect to the district’s network (wired and wireless). Any and all personnel that do not adhere to this policy may be subject to disciplinary action.

**PROCEDURES**

**Overview**

The purpose of this procedure is to ensure all computers connected to the Quitman County School District’s network have up to date end point security software installed and operational.

The District utilizes various enterprise level tools to protect the network and data from malicious

intent. End users are not permitted to circumvent or disable these protection tools. tools include:

1. Desktop Security Protection with automatic update services
2. Enterprise Gateway Security Protection with automatic update services
3. Managed gateway firewall software/hardware based
4. Intrusion Prevention
5. Electronic Mail SPAM Controls with automatic update services
6. Network equipment management including firmware updating services
7. Microsoft Update Management implemented
8. Technology Protection Device for Content Filtering

**Areas of responsibility**

District Computers
• District Technology Coordinator

Non-District Computers
• Owners of the non-district personal device

**Procedure details**

The Technology Coordinator will install and configure the antivirus program and end point security on all computers. The Coordinator will install and configure the antivirus program and end point security on all servers.

The Technology Coordinator will monitor all devices through a management console. Minor issues such as out of date computers or anti-virus policy errors will be address and attempted to be resolved during the weekly checks. If a virus is found or suspected users should shut down their computer and call the Technology Coordinator at (229) 334-9471 or submit a ticket via the technology department helpdesk system (Freshdesk)