NEOMIN Anti-virus Software Policy
February 20, 2002

1. Districts must have Virus Scanning software that has been approved by the NEOMIN Governing Board installed and operational on any device connected to the NEOMIN network.

2. Virus Scanning software must be updated on a daily basis, at a minimum.

Any buildings within a district that are found to be out of compliance with these two items will be subject to the following:

1st offense

An "Access Control List (ACL)" will be placed at the building's point of wide area connectivity to NEOMIN. Access control lists help provide a means for isolating the impact of any computer virus to the specific building that is restricted by the ACL. This ACL will restrict the type of network traffic that will function across the NEOMIN network.

ACL's that are implemented will permit the following type of activities:

- Access to primary system applications for fiscal, library, student services and EMIS users
- Email delivery systems
- Limited Internet connectivity

Before a building will be re-connected to the network or an Access Control List will be removed, written notification to NEOMIN would need to be submitted by the District Superintendent certifying that all devices within a specific building have:

- Been scanned for viruses.
- Had all new patches applied or software versions updated
- Reformatted any infected servers and/or PCs and reloaded with appropriate software, applicable patches and any data that the school may need

2nd Offense

The building will be disconnected from the NEOMIN network in order to maintain the integrity of the network for all NEOMIN schools. The building will remain disconnected from the NEOMIN network until a written plan of action to correct the problem(s) is submitted by the district and approved by NEOMIN management.

An "Access Control List (ACL)" will be placed at the building's point of wide area connectivity to NEOMIN upon re-connection to the NEOMIN network. This ACL will remain in effect for a period of at least 15 days upon reconnection.

3rd Offense

The building will again be disconnected from the NEOMIN network in order to maintain the integrity of the network for all NEOMIN schools. The building will remain disconnected from the NEOMIN network until a NEOMIN mandated solution for purchasing and implementing a virus scanning software solution is agreed to by the District and NEOMIN.

An "Access Control List (ACL)" will be placed at the building's point of wide area connectivity to NEOMIN upon re-connection to the NEOMIN network and will remain in effect until the NEOMIN mandated solution is implemented. All costs associated with a NEOMIN mandated solution will be the sole responsibility of the District and may include, but are not limited to the following:

- Purchase of Anti-virus software
- Purchase of hardware to be used to distribute updates of the anti-virus software within a specific building
- Labor for installing and configuring software on all devices within the specific building
- Labor associated with reformatting any infected servers and/or PCs and reloading with appropriate software, applicable patches and any data that the school may need

NOTE: NEOMIN can purchase Virus Scanning software on behalf of participating districts in order to maximize quantity discounts and minimize costs. Any costs associated with these purchases would be charged back to the participating schools.

The following anti-virus software packages are currently in use and should be considered as approved scanning software products as of 2/19/2002.

- Norton Anti-virus Software
- Sophos Anti-virus Software
- AVG Anti-virus Software
- McAfee Total Defense Suite
- Trend Micro Systems
- Command F-Prod for PC's and Intego for the Macs.