ACCESS Security Policy

ACCESS has implemented security application technology within the ACCESS wide area network. This technology detects potentially malicious traffic within the wide area network and provides reporting information outlining its findings. Findings indicating attention will be categorized into three levels with actions assigned to each level.

<u>Level I</u> - A device is identified producing significant malicious traffic to the detriment of the ACCESS network…

- Traffic from district device will be blocked by ACCESS.
- District will be immediately notified of the IP and/or host name of the device (computer) within their network causing the incident.
- ACCESS will reinstate device traffic once district has resolved the incident.

<u>Level II</u> - A device is identified producing malicious traffic to the detriment of either the ACCESS network or the district local area network…

- District will be immediately notified and ask to remedy the situation.
- If the situation escalates without resolution, the district will be re-notified and the device traffic will be blocked by ACCESS.

<u>Level III</u> - A device is identified producing traffic identified as Malware, Spyware, or Virus activity…

- District will be provided with the IP and/or host name of the device in question for proper resolution.

- If the Malware, Spyware, or Virus activity negatively affects the ACCESS network, the device traffic will be stopped at the ACCESS head-end district router preventing the traffic to traverse the ACCESS network. All malicious traffic will be contained within the district local area network until incident is resolved.

In an effort to assist districts in identifying potential Level I, II, and III threats, weekly e-mail messages will be sent to at least two district-identified contacts identifying (1) the type of threat posed by a certain computer, (2) the level of severity of the threat, and (2) the IP address and/or host name of the affected computer.