ACCESS Security Policy

Level Determinants

Level I

Determined activity includes, but is not limited to:

- ✓ Denial of Service Attack (DOS),
- ✓ Breach of security of any ACCESS application server.
- ✓ Excessive traffic traversing the wide area network originating at the district causing congestion on the ACCESS backbone impeding application services to all districts and ACCESS.

Level II

Determined activity includes, but is not limited to:

- ✓ Breach of security of one of the district servers – originating from within the ACCESS network or from outside the ACCESS network through trusted services (file sharing – video, music, etc.).
- ✓ Excessive traffic traversing the wide area network originating at the district causing congestion on the ACCESS backbone impeding application services to the district.
- ✓ Identifiable "attempts" of a device producing malicious traffic destined for an ACCESS application server.

Level III

Determined activity includes, but is not limited to:

- ✓ Identified viruses, Trojans, malware and spyware as outlined by the U.S. Computer Emergency Response Team (US-CERT - http://www.us-cert.gov) and detected by the ACCESS Intrusion Detection System (IDS).