NEOMIN NETWORK
SECURITY POLICY

1. NEOMIN does not currently provide any type of automated network intrusion detection system or any other tools for protecting systems owned and operated by districts in the consortium. It is difficult and sometimes impossible to trace the source of an attack after the fact; therefore, security measures must be taken in advance in an effort to proactively avoid system problems.

2. District personnel are exclusively responsible for system administration and system security on district-owned computers. On district-owned and operated systems, prevention of all types of malicious exploits including denial of service attacks, virus infection, tampering, unauthorized access, etc. is the sole responsibility of the district.

3. District personnel are exclusively responsible for keeping abreast of security issues related to their systems and the internet at large and taking measures to ensure system and data integrity and availability. Security is an ongoing challenge for all systems and network administrators in all networking environments, and especially on the Internet. NEOMIN recommends that systems be monitored continually.

4. District personnel are responsible for conducting regular system and data backups on district systems in accord with district policy in order to provide for system recovery in the event of system failure or a destructive malicious attack. NEOMIN is not responsible for data loss on district systems.

5. District personnel are exclusively responsible for educating all of their users concerning network security policies and issues, including district and NEOMIN acceptable use policies.

6. District personnel are responsible for contacting NEOMIN immediately if district personnel make changes to the configuration of the servers listed in this document in order to have changes made to the firewall configuration to maximize security and minimize exposure to malicious attacks from outside systems.

7. NEOMIN reserves the right, upon detection of a security threat associated with a district server, to immediately shutdown access to that server from outside hosts or to take whatever measures are deemed necessary to protect other systems inside the NEOMIN intranet. Advance warning of such a shutdown may not always be possible, but NEOMIN will make every effort to notify district personnel in advance or otherwise as soon as possible.

I have read the information above and attest that the security concerns on systems have been and will continue to be addressed within my district.

Signed,

______________________________________ ______________________________________

<DISTRICT NAME> Superintendent Date