June 10, 2003

Superintendents and Technology Coordinators,

In an attempt to improve overall network security and provide sufficient documentation to meet the network security requests of our auditors, the NEOMIN Governing Board adopted the enclosed “NEOMIN Static Map Application” as a supplement to our existing “Network Security Policy”. You are receiving these documents because your district has been providing or would like to begin providing a service(s) that will require changes to the security structure of the NEOMIN network. These changes include the establishment of a “static map” through NEOMIN’s Firewall.

In order to maintain your current service(s) or begin your new service(s), the following process will need to be completed:

1. Districts must review, understand and agree with the “NEOMIN Network Security Policy”.

2. District must complete a “Static Map Application”, have the Superintendent sign the document and either fax (330-847-8568) or mail the request to NEOMIN. (NOTE: A signed copy of the “NEOMIN Network Security Policy” should also accompany the application that is sent from your district.)

3. NEOMIN Management and Network Coordinator will review the application.

   Because of the serious nature of network security and the impact one exposed device could have on the entire NEOMIN network, approval of applications for exposure through NEOMIN’s firewall will be closely analyzed before approval will be granted. Some of the criteria that will be used to judge the merit of an application include:

   - Purpose of the request – what is the educational or economical purposes of the request
   - Security controls that are in place in the building and on the device
   - What risks or liabilities does the exposure of the device cause or what liabilities could arise if the service would be unavailable

4. NEOMIN management will either:
   a. Temporarily approve the application;
   b. Deny the application;
      i. The district will be notified in writing if the application is denied
      ii. If NEOMIN management denies the request, the district can appeal to the NEOMIN Governing Board. The board meets at least four times during each fiscal year.
   c. Request additional information via writing from the district.

5. If the application is approved by NEOMIN Management

   a. NEOMIN Network staff will establish a temporary static map through the NEOMIN firewall.
      i. The NEOMIN Governing Board will have final approval of all static maps established through the firewall.

6. **Approval of application does not guarantee firewall change is permanent**

   a. The NEOMIN Governing Board has the final authority in approving all applications and may overrule NEOMIN management's temporary approval.
   b. Access privileges will be revoked if:
      i. The NEOMIN Governing Board denies the request.
      ii. Devices do not have the proper software or system updates applied as they are released from vendors.
      iii. Updates to virus scanning software are not kept current.
      iv. Districts do not keep NEOMIN informed of any changes that are made to all exposed devices.
      v. Upon detection of a security threat associated with a district server
      vi. "NEOMIN Network Security Verification Form" is not completed and returned to NEOMIN by the start of the annual NEOMIN Audit. (see item 7)

   Note: Devices will be scanned by NEOMIN network personnel on at least a quarterly basis to verify software, operating systems and security controls are up to date.

7. The application process will be reviewed on an annual basis.

   a. Part of the review will include the completion of a "NEOMIN Network Security Verification Form". NEOMIN will create the form and mail it to each district superintendent on an annual basis. This form will need reviewed, modified as needed, signed by the Superintendent and returned to NEOMIN prior to NEOMIN's annual audit.

Please contact NEOMIN with any questions or concerns.

Thank you,

John Jaros
Executive Director, NEOMIN