Enterprise K12 Network Security Policy

I. Introduction

The K12 State Wide Network was established by MDE and ITS to provide a private network infrastructure for the public K12 educational community. Therefore, it is the sole privilege of each and every public school district to participate in the K12 network.

The purpose of the K12 Network Security Policy is to create an environment for MDE and the school districts to maintain system security, data integrity, and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data. Mississippi Public School Districts, utilizing the K12 Network, shall adhere to the policies identified in this document and use these standards in which to develop, implement, and maintain their own security plans pertinent to their scope of responsibility as defined in this policy. In addition**,** each district is responsible and accountable for its own security plan and should educate employees to follow security procedures. Technological advances and changes in the business requirements will necessitate periodic revisions; therefore, districts should review and update IT security plans at least annually or following any significant change to its business, computing, or telecommunications environment.

II. Policy Development

The K12 Network Steering Committee is composed of representatives of 14 school districts and MDE personnel. These representatives entered into discussions both in meetings and in an online forum to develop this policy. The ITS Network Security Policy was used as a framework, and was modified to address the specific needs and concerns of MDE and the school districts.

III. Purpose of the Security Policy

The state's transition from multiple proprietary network connections over dedicated leased networks to the Internet for conducting official business has highlighted the following security concerns:

- Information Integrity - Unauthorized deletion, modification or disclosure of information;
- Misuse - The use of information assets for other than authorized purposes by either internal or external users;
- Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users;
- Penetration - Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs;
- Computer Viruses – Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files or devices on a system or through multiple systems in a network, that may result in the destruction of data or the erosion of system performance;
- Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization;
- Component Failure - Failure due to design flaws or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component; and
- Unauthorized additions and/or changes to infrastructure components.

Because information technology security planning is primarily a risk management issue, this policy and its associated standards and guidelines focus on the creation of a shared and trusted environment, with particular attention to:

- Common approaches to end-user authentication;
- Consistent and adequate network, server, and data management;
- Appropriate uses of secure network connections.

Such an environment is made possible through an enterprise approach to security in the K12 community that:

- Promotes an enterprise view among separate districts;

- Requires adherence to a common security architecture and its related procedures;
- Recognizes an interdependent relationship among school districts, such that strengthening security for one strengthens all and, conversely, weakening one weakens all; and
- Assumes mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users.

In response to these threats and to assist school districts in mitigating associated risks, the Board of Education requires that districts take steps necessary to initiate an enterprise-wide approach to:

- Ensure secure interactions between and among governmental agencies and school districts take place
  within a shared and trusted environment;
- Ensure secure interactions between and among business partners, external parties, and school districts to utilize a common authentication process, security architecture, and point of entry;
- Prevent misuse of, damage to, or loss of MDE/District hardware and software facilities;
- Prevent unauthorized use or reproduction of copyrighted material by public entities.

Accordingly, the Board of Education directs MDE and Districts to:

- Operate in a manner consistent with the K12 Network Security Policy
- Develop, implement, maintain, and test security processes, procedures, and practices to protect and safeguard voice, video, and data computing and telecommunications facilities -- including telephones, hardware, software, and personnel -- against security breaches;
- Train staff to follow security procedures and standards;
- Apply appropriate security measures when developing transactional Internet-based applications, including but not limited to electronic commerce (e-commerce); and
- Ensure and oversee compliance with this policy.

IV. Security Policy Scope

For the purposes of this policy, security is defined as the ability to protect the integrity, availability, and confidentiality of information held by a district and to protect network assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of network facilities and off-site data storage; computing, telecommunications, and applications related services purchased from commercial concerns; and Internet-related applications and connectivity.

This policy applies to all educational institutions, as provided by law, that operate, manage, or use network services or equipment to support critical state business functions. The scope of responsibility for MDE shall include all network components from district-level routers throughout the K12 Network to its connection with ITS. A school district's scope of responsibility shall be from the district connection at said router throughout the entirety of the school district's wide- and local-area networks.

V. Security Policy Exemptions

This policy applies to Mississippi Public School Districts except when they develop security policies in lieu of the policy statements below
that are:

1) Appropriate to the school districts respective environments,

2) Does not adversely affect the remainder of the K12 Network, and

3) Consistent with the intent of the K12 Network policy. Such districts security policies must address:

   - Appropriate levels of security and integrity for data exchange and business transactions;
   - Effective authentication processes, security architecture(s), and trust fabric (s); and,
   - Compliance, testing and audit provisions.

VI. General Security Policy

It is the network security policy of the K12 educational community that:

1) Each district shall operate in a manner consistent with the maintenance of a shared, trusted environment within state government for the protection of sensitive data and business transactions. Districts may establish certain autonomous applications, including those hosted by Applications Service Provider or other third party, outside of the shared, trusted environment, PROVIDED the establishment and operation of such applications follows all guidelines as set forth in this security policy and does not jeopardize the enterprise security environment, specifically:

    - The security protocols (including means of authentication and authorization) relied upon by others; and
    - The integrity, reliability, and predictability of the State backbone network.

2) Furthermore, each district that operates its applications and networks within the Mississippi K12 Educational Network Infrastructure must subscribe to the following principles of shared security:

    - Districts shall follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels;
    - Districts shall recognize and support the state's standard means of authenticating external parties needing access to sensitive information and applications;
    - Districts shall follow security standards established for securing servers and data associated with the secure application; and
    - Districts shall follow security standards established for creating secure sessions for application access.

3) Each district should review its IT security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment. Examples of these changes include modifications to physical facility, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization, or budget. Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified by third parties.

4) Each district is responsible for the oversight of its respective districts IT security and will confirm in writing that they are in compliance with this policy. The annual security verification letter must be signed by the current Superintendent and submitted to MDE. The verification indicates review and acceptance of district security processes, procedures, and practices as well as updates to them since the last approval.

5) The State Auditor may audit district IT security processes, procedures, and practices. The State Auditor may audit any district for compliance with this policy.

District IT security processes, procedures, and practices may contain information (confidential or private) about the district's business, communications, and computing operations or employees. Policy and procedures for distribution of any related documentation should consider sensitive information and related statutory exemptions for such information from public disclosure.

VII. Security Policy; Review, Schedule and Updates

Technological advances and changes in the business requirements will necessitate periodic revisions; therefore, districts should review and update IT security plans at least annually or following any significant change to its business, computing, or telecommunications environment.

Districts should promote security awareness by informing employees, associates, business partners, or others using its computers or networks about security policies and practices, what is expected of them, and how they are to handle the information.

VIII. Web Server; Connectivity, Security, Physical Location

If a district maintains a web sever that resides on the State network and needs to be accessible from the Internet, there are several security guidelines that must be met. These include:

1) MDE will house a proxy server(s) inside the MDE firewall which will perform a reverse proxy service for every web server on the K12 network. All HTTP and HTTPS request from the Internet will be redirected through the MDE Firewall to the proxy server(s).

2) Each district is required to "harden" the server by making sure that all the current operating system patches are applied and kept up-to-date, removing any unnecessary server processes, etc., as recommended by MDE-MIS.

IX. E-mail; Functionality, Security, Limitations

For the purpose of security and limiting Spam into the network, MDE shall implement and maintain mail relays on the inside of the firewall. All mail entering and exiting the K12 network must come through the mail relay and be "relayed" to the appropriate mail server.

1) No direct SMTP from the Internet. Districts must utilize the MDE maintained mail relays for mail traveling in from the Internet.

2) No POP or IMAP from Internet to mail servers inside State network. Districts must utilize a web interface (HTTP/HTTPS) to access this mail.

3) Only the districts e-mail server will be permitted to have SMTP traffic pass from the district. All other SMTP traffic will be stopped at the district router.

X. Antivirus Software; Virus Prevention, Detection and Removal

There are several kinds of software that can surreptitiously breach computer and/or network security. They include:

• virus: a code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources, which are then not available to authorized users.

• worm: an independent program that reproduces by copying itself from one system to another, usually over a network. Like a virus, a worm may damage data directly, or it may degrade system performance by consuming system resources and even shutting down a network.

• Trojan horse: an independent program that appears to perform a useful function but that hides another unauthorized program inside it. When an authorized user performs the apparent function, the Trojan horse performs the unauthorized function as well (often usurping the privileges of the user).

A common method of sending these computer viruses is via email. MDE will scan all inbound email for viruses. Districts shall implement and maintain anti-virus software on their networks. MDE strongly recommends that all districts implement administrative policies in regard to virus and email. These should include:

1) Maintain real-time anti-virus software on the network including all servers and workstations.

2) Be diligent about keeping virus definition files up-to-date. The virus scanning software is only as good as the virus definition file associated with the scan. Virus scans performed with out-dated definitions file will not locate the newest, latest and greatest virus threat.

3) Instruct network users not to open attachments from individuals they do not know and/or trust. Instruct them to either delete the email in question or notify the support staff for further investigation.

4) Once a device is infected with a virus, the offending machine should be removed from the network until such time the virus can be removed from the machine.

5) Please note that copies of virus-detection and eradication tools should be kept offline. Otherwise it is possible that the virus could modify the detection tools to prevent its own detection. You should actively scan/check for viruses online, but periodically use the off-line, trusted copies of the tools to scan your systems.

XI. Firewalls Requirements; Use, Functionality and Port Restriction

MDE will maintain a firewall within the core of the network that provides one level of protection of the State network from the connection to the Internet. Below are examples of what will not be permitted:

1) No direct SMTP from the Internet. Districts must utilize the MDE maintained mail relays for mail traveling from the Internet.

2) No POP or IMAP from Internet to mail servers inside State network. Districts must utilize a web interface (HTTP/HTTPS) to access this mail.

3) No FTP access allowed from Internet to a device on K12 network.

4) MDE will not restrict FTP out of the State network to a device on the Internet provided that session/transfer is initiated from the State network.

5) No LAN protocols mapped to and/or from devices on Internet (i.e. NetBios, NetBeui, NFS, etc.).

6) No ICMP to and/or from Internet to State network.

7) Any outbound port that has the potential of propagating industry-known viruses, worms, etc.

The exception to these port restrictions is when a district has a VPN implemented between them and a third party. In that scenario, all ports are available for use provided the traffic goes through the VPN.

AT NO TIME may a district permit a third party entity to connect directly to their local area network behind the State's firewall . **This backdoor direct connection is a serious security violation.** This includes terminating third party circuits behind MDE firewalls and/or utilizing a PC remote control product (i.e. PCAnywhere) and a modem over a dialup connection.

XII. Non-State-Business Related Network Traffic

Bandwidth has a high cost associated with its usage. The State network was implemented and is maintained to allow state and district employees to utilize automated systems and tools to help facilitate their carrying out work responsibilities and duties and meeting the needs of those individuals they serve. In saying that, the State network infrastructure must not be utilized for personal gain and/or entertainment. Unnecessary applications that pose potential security risks will not be permitted on the State network. These include, but are not limited to:

1) Instant Messaging protocols outbound from State network to Internet will be permitted. However, the ports that these applications use can be used to hack into systems or these applications can be used as a means to download viruses, worms, etc., therefore any district may request that these protocols be blocked on an individual basis.

2) Music/video/file sharing services (I.e. Napster, Kazaa, etc.) and any other illegal software or services will not be permitted on State network. In addition to security concerns, these services

are bandwidth "monsters". Also there are legal ramifications that are tied to users who use these applications to share files.

XIII. Wireless Access Connectivity

Due to the security issues that are present with wireless connectivity, any district that will use wireless technology for their local and wide area connectivity shall enable and configure the highest form of Wired Equivalent Privacy (WEP) encryption and some type of authentication method (i.e. VPN, radius) on all wireless devices.

XIV. Internet Filtering

MDE has Internet filtering servers located at the core to provide content filtering for districts who wish to utilize this service. Districts using this filtering service will be compliant with filtering component of CIPA regulations. Any district that is not being filtered by these servers MUST provide their own filtering to be compliant with CIPA regulations.

XV. Application Service Providers

MDE has VPN concentrators located at the core, which can be used to grant vendors access inside the K12 network to the district site as needed. If it is deemed necessary to have a vendor directly connect to the district network to support an application or service, this will be permissible as long as the following are met:

1) MDE/MIS will be contacted before any connection is granted;
2) District will take appropriate steps for additional security (firewall, access-list) on their network;
3) Vendor has taken appropriate steps for security on their side of network; and,
4) Vendor will sign agreement stating the connection will ONLY be used for support for that particular district.

In the event that unauthorized activity by the vendor is noted outside the supported districts WAN, MDE shall have the authority to take appropriate action at its discretion. Including, but not limited to, blocking access to the K12 network from that district.

XVI. Conclusion

It is the goal of MDE and the K12 Network steering committee to have 100% compliance for all districts utilizing the K12 network. In order for this goal to be met, each district must be given time to examine their own processes and procedures, and if any guidance is needed from MDE, make the appropriate changes necessary to conformed with this given policy. Any new process or procedure that a district is getting ready to implement needs to conform to the security policy.