DRAFT

M-DCPS SCHOOL SITE SECURITY AUDIT CHECKLIST

School ____ Principal _____ Tech _____ Date _____

The following items should be printed off and available for review by the auditor:

- ❑ Screen print of local Domain and/or Organizational Unit (OU) Group Policy settings for user accounts and passwords demonstrating district standards are being met.
- ❑ Most recent RACF Authorizations Quarterly Report for the location with site administrator's signature indicating that they have reviewed the report.
- ❑ Principal's proof that they have copies of all Domain Administrator passwords in their possession and stored securely.
- ❑ Count of all computers actually at school and E-Policy Orchestrator (EPO) count of computers with anti-virus administered by EPO (EPO report "Product Protection Summary Report"). Difference in count should be explained (some computers are Apple Macintosh, other computers not hooked to the network, etc).
- ❑ Recent EPO Data Definitions should be in place (EPO report "DAT/Definition Deployment Summary").
- ❑ Screen prints demonstrating that all Wireless Access Points have most recent patches and all security features configured (encryption, default SNMP password changed, only computers in list allowed to connect, broadcast feature turned off so that the Access Point is not advertising its presence, etc). See "Wireless Security Tech Note" at

  http://techsupport.dadeschools.net/data_security/wireless_security.pdf
- ❑ Screen print demonstrating Electronic Grade-book security features are turned on. Auditor may ask for demonstration of how a teacher signs in.
- ❑ Screen prints demonstrating all servers have proper configuration and are up-to-date with patches for the Operating System and Internet Explorer. Other applications on the server must also have most recent updates.
- ❑ Screen prints demonstrating routers, hubs, switches, etc. have updated software.
- ❑ Screen prints demonstrating that all Guest accounts have been disabled and individual users receive authorizations via group membership, not as individuals. Default Administrator passwords should have been changed.
- ❑ Screen print of all domain controllers indicating that the MDCPS Enterprise Administrators are members of the Administrators group and Domain Administrators Group.

In addition to the above documentation, auditor should also spot check as follows:

- ❑ Auditor should check on physical security of servers, hubs, switches, routers, etc (locked room with limited access, protection from elements, free of risk from leaks from plumbing, air conditioning, rain, etc.).
- ❑ Tech should have hard copy of the Network Security Standards and other district security policies or demonstrate they know where to find it (see

  http://techsupport.dadeschools.net/data_security/datasecurity.htm

- Auditor should check that tape backups are regularly scheduled and that the backup tapes themselves are physically secure in the event of a disaster. All important data and documents should be included in the backup. OS media and other necessary server software should also be physically secure and ready in case of a needed disaster recovery. The backup server should itself be backed up and so should server system states. Disaster Recovery Procedures should be documented.

- Procedures and standards should be documented and available for viewing.

- Proof of licensing for all software at the location should be should be organized and available for viewing. There should be enough licenses of each software package to cover use at the site based on the requirements of each license agreement.

- Auditor should check on physical security of main office (limited access to administrative computers by parents, students, and other unauthorized personnel). Computers in administrative areas should have screensaver and/or start-up passwords on.

- Auditor should spot check some desktops to ensure up-to-date patches have been applied and EPO is updating anti-virus. For PC's, the bare minimum for updates are Windows and Internet Explorer.