

MEMORANDUM

June 27, 2008
AMV 2007-2008/M118
AMV 305-995-1436

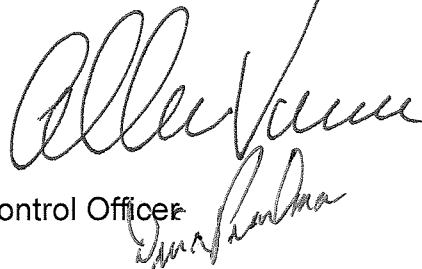
TO: All Principals

FROM: Allen M. Vann, Chief Auditor
Office of Management and Compliance Audits

BY: Dina Pearlman, Information Systems Design Control Officer
Office of Management and Compliance Audits

SUBJECT: **SCHOOL SITE INFORMATION TECHNOLOGY SECURITY AUDIT**

Due Date: **September 30, 2008**



The attached document is a self-assessment survey of IT security practices at school locations. The importance of IT security practices is a direct reflection of the increasing reliance the District places on technology and the infrastructure that supports it. In order to continue moving towards the safest and most secure network possible, the Office of Management and Compliance Audits (OMCA), in collaboration with ITS, has developed this survey assessment to ensure that District data and technology assets are protected.

The issues addressed in this survey are based on current industry best practices and the District's Network Security Standards, published by ITS and available on the ITS website. The Network Security Standards document should be reviewed by school administrators and adhered to by all school staff and technology support personnel. The policies and procedures outlined in the Network Security Standards document should currently be in effect at all locations.

This survey of IT security practices must be completed and returned to OMCA, and will provide the baseline for a technology based audit of the school site. Based on specific risk assessment criteria, certain schools from each region will have the technology audit portion included in their annual school audit, to be conducted concurrently with that audit.

The top portion is to be completed by the work location administrator. The remainder is to be completed by your technician. A fillable form version of this assessment is available on the OMCA website at <http://mca.dadeschools.net/itaudits/it.asp>. When the assessment is complete, please print it out. Both the work location administrator and the technician should sign the survey. **The form can then either be scanned and e-mailed to Dina Pearlman (pearlman@dadeschools.net) or faxed to the OMCA at 305-995-1331, attention Dina Pearlman.** The original should be kept in the work location files.

If you have any questions please feel free to contact either Dina Pearlman at 305-995-4795, or Luis Baluja at 305-995-7575 or via e-mail:

pearlman@dadeschools.net | luisbaluja@dadeschools.net

The form below is "FILLABLE"



OFFICE OF MANAGEMENT AND COMPLIANCE AUDITS SCHOOL SITE IT SECURITY ASSESSMENT (2008-2009)

WL Name: _____ WL #: _____ DATE: _____

If your location is selected for an IT audit, you may be asked by an Auditor to demonstrate any procedure or provide documentation. If discrepancies exist, please provide a written explanation in the space provided on the next page. Please refer to Weekly Briefings (WB*) and Network Security Standards (NSS**) as noted. For further information and relevant links, please visit <http://mca.dadeschools.net/itaudits/it.asp>.

ITEM	DESCRIPTION	YES	NO
WORK LOCATION ADMINISTRATOR (PRINCIPAL)			
1	Principal has reviewed, signed, and filed the most recent RACF Authorizations monthly report. (Product T0802E0101) (WB #1120 * and NSS 5.0 **)	<input type="checkbox"/>	<input type="checkbox"/>
2	Principal has all LOCAL administrator passwords in their possession, stored securely, and has shared the location of the passwords with Assistant Principal(s). (NSS 5.1 **)	<input type="checkbox"/>	<input type="checkbox"/>
3	Only appropriate personnel have access to input or change grades within the Electronic Grade Book. (WGBM / WGBA) (NSS 4.1.4 **)	<input type="checkbox"/>	<input type="checkbox"/>
4	Only administrative personnel (Principal / AP) can approve payroll. (RSTR) (WB #3833 *, and NSS 4.1.4 **)	<input type="checkbox"/>	<input type="checkbox"/>
5	5a. Does your work location house any non-MDCPS agencies, such as a clinic, using computer equipment not owned by MDCPS?	<input type="checkbox"/>	<input type="checkbox"/>
	5b. If you answered YES to 5a and the agency-owned equipment is connected to the MDCPS network, does all connected equipment conform to MDCPS security standards? (Consult with your school base technician.)	<input type="checkbox"/>	<input type="checkbox"/>
	5c. If you answered YES to 5a and the agency-owned equipment is NOT connected to the MDCPS network, does the equipment conform to MDCPS student access and site filtering requirements? (Consult with your school base technician.)	<input type="checkbox"/>	<input type="checkbox"/>
6	Only the Principal, AP and Registrar have access to change grades within ISIS (ISIS-ACAD GRD/TRACE UPD) or VACS (VACS-GRADES & HRS UPDT). (NSS 4.1.4 **)	<input type="checkbox"/>	<input type="checkbox"/>
7	Servers, switches, routers, etc., are secured (locked room with limited access, protection from elements, free of risks from plumbing leaks, air conditioning, rain, etc.). (NSS 3.0 **)	<input type="checkbox"/>	<input type="checkbox"/>
8	The Principal has reviewed the MDCPS Network Security Standards (NSS) with the SBT. (NSS 5.0 **)	<input type="checkbox"/>	<input type="checkbox"/>
9	Proof of licensing for all installed software is centrally organized and available for review. A staff member has been assigned to coordinate all license management. (NSS 5.0 **)	<input type="checkbox"/>	<input type="checkbox"/>
School Based Technician (SBT)			
10	All servers are properly configured and up-to-date with patches for the Operating System, Internet Explorer, and other software. (NSS 4.1.1 **)	<input type="checkbox"/>	<input type="checkbox"/>
11	Patch management software (BigFix) and licensed antivirus software are installed on all machines. (NSS 5.0 **)	<input type="checkbox"/>	<input type="checkbox"/>
12	All computers (including MAC OSX or above) have been migrated (bound) to the DADESCHOOLS domain. District standards are being met for local Domain and/or Organizational Unit (OU) Group Policy settings for user accounts and passwords. (NSS 4.1.1 **)	<input type="checkbox"/>	<input type="checkbox"/>
13	All non-ITS managed wireless access points have the most recent patches and available, security features configured (encryption enabled, default passwords changed, broadcast feature disabled, etc.) (NSS 4.2 **)	<input type="checkbox"/>	<input type="checkbox"/>
14	All Guest accounts have been disabled and users receive authorizations via group membership, not as individuals. Default Administrator passwords have been changed. (NSS 4.1.1 **)	<input type="checkbox"/>	<input type="checkbox"/>
15	Domain Administrators are members of the Local Administrators group. There is no systematic or random removal of these members. (NSS 4.1.1 **)	<input type="checkbox"/>	<input type="checkbox"/>
16	All computers are named appropriately, starting with the work location number. (EX: 9131-123ABC)	<input type="checkbox"/>	<input type="checkbox"/>



**OFFICE OF MANAGEMENT AND COMPLIANCE AUDITS
SCHOOL SITE IT SECURITY ASSESSMENT (2008-2009)**

WL Name: _____ WL #: _____ DATE: _____

ITEM		YES	NO
School Based Technician (SBT)			
17	The work location has an operational District-approved intrusion prevention device on the network. (EX: Tipping Point) (NSS 5.0 **)	<input type="checkbox"/>	<input type="checkbox"/>
18	Main office computers are physically secured (limited access to administrative computers by parents, students, and other unauthorized personnel). (NSS 4.1.1 **)	<input type="checkbox"/>	<input type="checkbox"/>
19	The location has diagrammed documentation indicating how the network is physically configured (i.e., location of servers, switches, router, etc.)	<input type="checkbox"/>	<input type="checkbox"/>
20	A documented disaster recovery plan is available for review. (NSS 4.1.1 **)	<input type="checkbox"/>	<input type="checkbox"/>
21	Non-ITS managed servers (local) are being backed up weekly. (NSS 4.1.1 **)	<input type="checkbox"/>	<input type="checkbox"/>

_____ Count of computers actually present at location

Please use the space below to provide explanation or clarifications regarding any of the audit items listed in this assessment:

Printed Name of Principal

Signature of Principal

Date

Printed Name of Technician or Alternate

Signature of Technician or Alternate

Date