M E M O R A N D U M October 24, 2008

TO: Superintendent's Senior Staff
All School Principals
All Non-School Site Administrators

FROM: Alberto M. Carvalho, Superintendent of Schools

SUBJECT: M-DCPS NETWORK SECURITY STANDARDS REVISION

The M-DCPS Network Security Standards are revised as often as necessary to ensure a high level of protection for the District's data assets.

Since the last update, a number of issues have made revisions to these Standards necessary. Some of the changes include:

- Computers with Windows 9x or older Operating Systems are prohibited from being connected to the District's network, as the inherent weaknesses in these systems pose a threat.
- A new section limiting the numbers of school staff members given specific, highly sensitive access has been added.
- Users with access to confidential systems and data must log off or lock their computers when leaving them unattended.
- Any confidential data placed on laptops, jump drives, removable media like CDs, etc. must be encrypted, redacted, or otherwise sterilized in case the device/media is lost or stolen.
- Only Apple iPhones with firmware version 2.0 or higher and specific settings can be connected to the system.
- Many new office copiers have hard drives and wireless capabilities just like computers and a section has been included describing the risks they may present.
- Use of Skype and other Voice Over IP (VoIP) applications are prohibited unless authorized; as these applications consume a great deal of bandwidth, which is becoming more expensive for the District because the recent state budget cuts have further reduced the state's share of the cost.
- Power Management requirements are listed.
- A link to the Office of Management and Compliance Audits' Web page, which includes the School IT Audit Assessment (Fiscal Year 0809), is provided.
- A number of sections have been re-organized to improve clarity.

These revisions have been extensively reviewed by representatives from the Office of Management and Compliance Audits, ITS Network Services, Instructional Technology Services, and selected M-DCPS network administrative staff from the District. In addition, external organizations such as the Gartner Group, InfoTech, and Ernst & Young also contributed to these revisions.

Your full compliance with all District security initiatives and Standards is required to keep our networks secure. It should be noted that acceptance of employment or contracts with M-DCPS will signify acceptance of these Standards by the user. Failure to comply with this or any M-DCPS computer security policy or standard may result in termination of employment, termination of contract, and/or prosecution.

Clarification or assistance is available by submitting questions via the e-Help Desk at:
http://sus.dadeschools.net/helpdesk/

Select "Ask a Question" from the drop-down list.

AMC:DCK:jod
M156
Attachment

Miami-Dade County Public Schools'
Network Security Standards - Administrative Summary

1.0 Data Classification and Security Objectives

Miami-Dade County Public Schools (M-DCPS) realizes that information is a valuable asset and must be protected from unauthorized destruction, access, modification, disclosure, loss, theft, or removal. These standards, in conjunction with appropriate state and federal statutes, will serve as a foundation for the protection of M-DCPS data. All security measures must conform to established M-DCPS policies and applicable federal, state, and local laws.

Sections 1.0, 1.1, 1.2, 1.3, 2.0, and 2.1 provide the basis of a data classification policy by laying out scope, risks, and goals. In addition, Sections 5.0 and 5.1 lay out specific user responsibilities regarding the protection of District data and should also be viewed as part of the District data classification policy. Sections 3.0, 4.0, 4.1, and 4.2 provide a detailed technical roadmap to achieve these objectives, while sections 6.0 and 6.1 discuss changes to these standards.

1.1 Overview

M-DCPS has for many years relied on computers and data processing facilities to store and manipulate vast amounts of data. That data includes, but is not limited to, student records, personnel records, business, and accounting records. The explosion of networks and Internet related informational activities means that this sensitive data is more conveniently available to authorized staff in ways undreamed of even a few years ago but is also at risk. M-DCPS must address the issue of the security of this data in such a way that all avenues of access are strictly controlled and that the privacy and value of the data are not compromised.

The Office of Management and Compliance Audits (OMCA), in concert with ITS, reserves the right to audit M-DCPS locations for compliance with these Security Standards.

1.2 Risks to M-DCPS

Any breach of data security could be costly to school system staff, users, and students as well as the school system itself. Moreover, any number of individuals/agencies could improperly benefit from M-DCPS data. The following is a list of some of the technical risks:

- Altered data
- Stolen and intercepted data
- Data rendered inaccurately
- Destroyed data

- Loss of M-DCPS' ability to process data

The following is a list of some of the business risks to M-DCPS:

- Lawsuits for not protecting sensitive data
- Loss of funding (for example, FTE) due to the transmission of incorrect data to other agencies
- Unfair penalty or advantage to students due to the transmission of incorrect data (for example, incorrect transcripts resulting in unfair penalty or advantage to students applying for college and/or scholarships)
- Loss of negotiating or advantage by unauthorized disclosure of lists and other business assets to vendors
- Liability for incorrect data (including State and Federal penalties)
- Errors in business decisions due to inaccurate data
- Negative publicity surrounding the use of incorrect data and subsequent regulatory enforcement
- Inability to process business transactions in a timely fashion or not at all

Sensitive data is defined as any data that should only be viewed by authorized personnel. Data sensitivity is determined by, but not limited to, federal and state laws (including privacy acts), M-DCPS Board Rules, and decisions by senior staff and/or the data owners (see section 2.1 of this document).

1.3 Background of M-DCPS Data Security

Historically, almost all M-DCPS data was kept on the M-DCPS mainframe at Information Technology Services (ITS) and access was strictly controlled through the use of the mainframe IBM OS/390 Security Server[1] (RACF). As long as valuable data is kept on the mainframe, this accepted tried-and-true method of protection will continue to be the mainstay of our mainframe security efforts. Moreover, it provides a model hierarchical protection scheme, which can be used in an expanded network security paradigm. This includes the delegation of local authorization duties to an approved supervisor at the site. Approved supervisors include school principals and department heads.

2.0 Scope

In this document, authorized staff will hereafter be defined as all M-DCPS employees, consultants, vendors, auditors, students, temporary help, and others authorized by M-DCPS to use the specific M-DCPS computer systems, applications, and information required for the performance of their job or function. These specific functions are determined and/or approved by the site supervisor. Modification of authorizations without the site administrator's approval is prohibited.

The following is a list of some of the individuals/resources the Network Security Standards apply to:

- All authorized staff, volunteers, students, and vendors as well as unauthorized parties seeking access to M-DCPS computer resources
- All M-DCPS mainframes, minicomputers, personal computers, outside timesharing services, outside suppliers of data, network systems, wireless devices, M-DCPS-licensed software, and computer workstations
- All M-DCPS data and reports derived from these facilities
- All programs developed on M-DCPS time or using company equipment
- All terminals, communication lines, and associated equipment on M-DCPS premises or connected to M-DCPS computers over physical or virtual links

All M-DCPS staff and authorized non-staff must be aware of the risks and act in the best interest of M-DCPS. These standards detail staff's responsibilities for computer security. Unauthorized persons who attempt to use M-DCPS computer resources will be prosecuted to the fullest extent possible.

2.1 Owners of Data

All computer files and data are to be associated with a user. In general, unless otherwise specified, the head of the department who requested the creation of the files and programs that store and manipulate the data on the computer is the owner of the data. The owner is responsible for specifying whether the data is sensitive and which user-ids will be authorized to access it, or who will be responsible for giving such authorization.

3.0 Physical Security

Adequate building security (both physical and environmental) must be provided for the protection of all physical and logical M-DCPS computer assets and especially sensitive applications and data. Security includes, but is not limited to, lockable doors and windows, limited access, protection from water and the elements, alarms, access controls, and surveillance devices such as cameras and monitors. Site supervisors must protect all hardware and software assigned to their location. Administrative computers must be segregated from classroom computers. Students and unauthorized personnel should never have access to administrative machines.

4.0 Non-Mainframe System Security

Non-mainframe systems (Local Area Network (LAN) and Wide Area Network (WAN)) must have the same protection methodology in place as do mainframes to ensure M-DCPS computer assets are secure.

Programmatic methods are to be used to control access to non-mainframe resources. These methods include defining specific users or groups to specific system resources,

and use of the “least privilege” concept for access to all system-level resources such as the operating system, utilities, and databases. “Least privilege” is defined as a default of no access to these resources and the requirement of explicit permission and authorization by the owner based on need.

Non-Mainframe systems must be provided with

1. Auditing/logging of such security-relevant information as log-on information, resource access, and TCP/IP addresses whenever possible
2. Security modifications and system administrator events
3. Ability to audit /log specific users and resources on demand
4. Ability to send specific security sensitive events directly to a specified administrator’s workstation, terminal, or e-mail, preferably with an audible alarm

4.1 M-DCPS Network Systems Security

Network systems include any local area network (LAN)[2], wide-area network (WAN)[3], dial-up, Internet, servers, server connections, hubs, routers, lines, software, and data that are outside the M-DCPS mainframe system. The security must include both physical and logical layers of protection. As M-DCPS moves from storing and transferring sensitive information used within the M-DCPS in a “closed” network architecture utilizing private and/or leased lines to an “open” network architecture using Internet and TCP/IP network[4], employees must pay particular attention to the security of these assets.

4.1.1 Network Structure, Hierarchy, and Requirements

1. As a statement of direction, all administrative PC-type servers in M-DCPS should migrate to the Windows 2000 (or above) operating system. Microsoft no longer supports Windows NT and will not provide fixes or reports for vulnerabilities, including any new ones found. All servers still using Microsoft Windows NT must be migrated to a newer Windows server platform immediately. Administrators of servers currently using Novell, or any other PC network operating system should also strongly consider migrating to Windows 2003 Server. Desktops should similarly be migrated to Windows 2000 or above when possible to take advantage of higher levels of security.
2. Windows 2000 and beyond employs Active Directory Services (ADS), a hierarchical process similar to a pyramid. ITS has established and maintains the Windows 2000 root ADS (the top of the pyramid) for M-DCPS and determines local and group policy settings. In Microsoft terms, this structure is best described as a forest. All other District servers will be added to the ITS established Active Directory forest.
3. Below the root in the forest are Organizational Units (OUs) that are the school and administrative sites in the District. These local OUs are simply smaller networks with their own Domain Controllers (DC) that connect to the

M-DCPS network. These DCs are under ITS authority and are not to be managed in any way by the local OU administrators. Local OU administrators must strictly limit access to their OU from other OUs as well as the outside. ITS must have Enterprise Administrator rights to all OUs in the District forest. ITS must provide advanced notification of group policy changes.

4. Computers with Windows 9x or earlier are prohibited from being connected to any M-DCPS network. The security features of this level of Operating System (OS) are extremely primitive and leave user accounts vulnerable to a variety of risks, including unencrypted caching of user-ids and passwords. Microsoft does have a supported, secure, stripped-down version of Windows XP called **Windows Fundamentals for Legacy PCs** that can be used to replace Win9x. It provides browser functions and Active Directory authentication, although it has very limited support for full-blown applications like Office (see the Microsoft Web site for details).

5. All locations must migrate from the original school and District networks to the new dadeschools network. Most of these are old networks with weak security and must be removed from production immediately.

6. M-DCPS Board rules/directives/standards regarding the following topics must be read and followed at all times:

   M-DCPS "Acceptable Use Policy for the Network" policy

   http://www2.dadeschools.net/schoolboard/rules/Chapt6/6A-1.112.pdf

   M-DCPS Board Rules regarding Copyright

   http://techsupport.dadeschools.net/Copyrights-Policies/4c-1.06.pdf
   http://techsupport.dadeschools.net/Copyrights-Policies/4c-1.061.pdf
   http://techsupport.dadeschools.net/Copyrights-Policies/4c-1.062.pdf
   http://techsupport.dadeschools.net/Copyrights-Policies/4c-1.063.pdf

   M-DCPS Board Rule regarding staff use of District e-mail systems

   http://www.dadeschools.net/schoolboard/rules/Chapt4/4c-1.064.pdf

   M-DCPS Board Rule regarding student use of District e-mail systems

   http://www2.dadeschools.net/schoolboard/rules/Chapt5/5c-1.09.pdf

   The Office of Management and Compliance Audits (OMCA) web site, which includes the School IT Audit Assessment

   http://mca.dadeschools.net/itaudits/it.asp

7. Each department or school must maintain a disaster contingency plan to provide for recovery of data in case of catastrophic loss. At minimum, all M-DCPS data must be backed-up once a week, and all mission-critical data must be backed-up daily. Data on the backup media will be verified as usable.

8. Administrative computers are defined as non-classroom computers on which M-DCPS requisition and business functions, exempt student academic and demographic data, staff e-mail directives, staff tasks, etc. are stored and/or viewed. These computers should be kept physically and virtually separate from instructional computers. Students are not to have access, either physical or virtual, to production servers or any administrative computers.

9. Every effort should be made to secure classroom machines on which student testing, test grading and evaluation, grade book activities, and staff e-mail functions are carried out. This includes installing application passwords and timeouts, up-to-date anti-virus software, separate computers for teacher use only, the most current version of the District's patch-management software to ensure the computer has the most recent software and operating system security patches, installation of anti-spyware applications when available, possible storage of grade and test data on removable media, and limiting unsupervised student access as much as possible. Individual student accounts or common student accounts (STUDENT01) should be separate from teacher accounts.

10. All administrative computers and server consoles that are used to access or control sensitive data must have a screen saver timeout and password after a specific period of inactivity or some other lockout mechanism to prevent unauthorized persons from accessing the data via the logged-in user's account. The Windows timeout with password is available even if the specific application does not have one. Users should also be in the habit of locking their computer or logging off when they are finished or leaving the computer unattended, even for a brief time (See section 5.1.3 in this document). These computers may also have boot-up passwords.

11. Classroom computers are defined as computers used by students or servers that connect instructional computers. There are to be no administrative applications, especially mainframe sessions, installed on any of these computers or servers.

12. Outside access to M-DCPS networks should only be through "hardened" Web servers. This means that Web servers should have no other applications running on them and should not connect easily to the rest of the M-DCPS network. Information on Web pages must be kept as current as possible.

13. Access to critical resources should be managed by assigning individuals to a group. The group should be set up with the authority necessary to do the specific job/task or access specific data. This will provide management with a more efficient method to remove access authority when a user no longer is responsible for performing the task. Group membership should be reviewed on a regular basis to ensure all members are appropriate. Under no circumstances should users be assigned data folder or application rights as an individual, except for home folders.

14. Locations maintaining their own network components must keep diagrammed documentation indicating how the network is physically configured (i.e., location of servers, switches, routers, etc.).
15. All software that restricts, prevents or inhibits updates sent by ITS, including, but not limited to Deep Freeze, Fortress, Clean Slate, HD Guard, and others of this type are not to be installed without written permission from ITS.
16. No form of “Wake On Lan” (WOL) tool should be used to automatically turn on computers unless it is for immediate maintenance purposes, such as imaging. The use of this type of a tool undermines the purpose and effect of the new Power Management Program, which is a District-wide initiative that will save millions of dollars and help reduce emissions (See 5.0.17). In addition, local power management settings on PCs should only be altered by ITS.

4.1.2 Data Access, Transfer and Communication

1. Firewalls are servers that function as a barrier preventing unauthorized outside access to the M-DCPS network. Exceptions requiring access from the outside must be documented by filling out ITS's *Remote Client Support Agreement IP Entry (FM-6045)* (old), or either of the new *VPN/Dial-Up Access Request* forms (FM-6629, for vendors or employees). ITS will keep firewall audit logs and review them regularly for illicit activity against the firewall.
2. Access to secure mainframe applications via the network requires RACF authorization.
3. Dial-in to the M-DCPS network requires network authorization and access authentication.
4. The use of Remote Access Services (RAS) such as Digital Subscriber Line (DSL), dial-in technology with a modem, is prohibited unless authorized by ITS. This provides a "back door” around network security by giving users a direct connection to a remote server. If remote access is authorized and sensitive/confidential data is to be transmitted, the line must be secured by Virtual Private Network (VPN), Secure Socket Layer (SSL), or some other technology that encrypts the data so that it is never transmitted in clear text. Hackers using “sniffer” technology often scan transmission lines looking for data they can use. Examples include user-ids and passwords, account numbers and financial information, student data deemed exempt from public release by state law, or Human Resource (HR) data.
5. The use of communications software that provides the ability to remotely "take over" a network connected PC is prohibited unless authorized by ITS. If it is used, it should be strictly controlled by the local administrator and user. It should be turned on only when support is needed (and the

user has given permission, if applicable) and immediately turned off once the support has been provided.

6. Confidential data taken from the District, whether via laptop, jump drive, removable media like a CD or floppy disk, PDA, e-mail, FTP, printed report, or any other method, must be encrypted, redacted, or otherwise sterilized so if the content falls in the wrong hands it cannot be misused. Agencies outside the school system's secure "cloud" that engage in File Transfer Protocol (FTP)[5] operations or e-mail transmission with the District in which confidential data is transferred are to be encouraged to utilize an encryption process requiring asymmetrical (public and private) keys, such as PGP (Pretty Good Privacy). Transfer of confidential data and any exceptions to the encryption process must be authorized by ITS.
7. Application software that has built-in security functions must have these functions activated when this software involves confidential data. In addition, new software purchased to handle confidential data should have security capabilities as documented in sections 5.1 Userids and Passwords and 4.0 Non-Mainframe System Security.
8. Users should be aware that unprotected folders on the network are prey to many different forms of hacking. It is the responsibility of the local site administrator to ensure that this data is secure.
9. Network Administrators, including ITS staff, are prohibited from viewing or otherwise manipulating user files on the users' local drive without the permission of the user or the approval of appropriate administrative, legal or police staff unless there is a critical need to do so. Critical need is defined as faulty system function, virus activity, illicit hacking or Internet activities, pornographic or other offensive material activity, or other violations of District policies. These policies include, but are not limited to, the Internet Acceptable Use Policy, the E-Mail Policy, the Copyright Infringement Policy, the Network Security Standards or any other District policy, Board Rule or directive relating to user conduct. It should be noted that the District E-Mail Policy discusses the lack of privacy in the e-mail system at length.
10. Personal or vendor-owned devices such as desktops, laptops, Personal Digital Assistants (PDAs), etc., or portable/removable storage devices/media such as Universal Serial Bus (USB) jump drives should not be connected to any M-DCPS network without network administrator/site supervisor approval. These devices may carry applications, configurations, viruses, etc. that pose a risk to the network or may be used to remove sensitive data from the network. School system technicians may grant approval after, as time permits, certifying the device is not a threat to District networks. Technicians are not required to bring the personal device into compliance unless directed to do so by their supervisor. For more information, see 4.3 Portable Devices. ITS reserves the right to disconnect, modify and/or confiscate any device connected to the District network that does not meet these Standards, is being used

inappropriately, is not authorized, or poses a threat to any District data, network, or user.

11. Devices like routers, hubs, switches, firewalls, wireless access points, other network devices, modems, whether personally or District owned, should not be installed without prior approval from the site supervisor and ITS. Once approved, technicians are required to bring these devices into compliance with these Standards. ITS reserves the right to randomly scan or monitor for the presence of insecure, unauthorized, or corrupted devices connected to M-DCPS networks. As mentioned previously, ITS will disconnect, modify and/or confiscate any device not meeting these standards or that is being used inappropriately.
12. Sensitive/confidential data to be accessed via the Internet must be secured during transmission using encryption, 128 bit or higher if possible. This is most commonly done using SSL certificates which may be purchased from recognized certificate authorities on the Internet (See item 4, section 4.1.2 Data Access, Transfer and Communication).
13. Computers removed from service in the District must have the hard drives degaussed, re-formatted, or otherwise cleared of software and data before they can be sold, given away, or disposed of. District-licensed software, confidential data, user-ids, passwords, and information that can be used to access M-DCPS network and/or mainframe systems left on these machines may fall into the wrong hands if steps are not taken to eliminate it.
14. Staff must be aware that technology is constantly evolving and changes may pose new threats in areas that previously were not an issue. Copier and printer technology has evolved to the point where there is wireless communication to these devices from computers and hard drives/solid state memory within the device may hold copies of all documents printed/ copied/ faxed. This means that wireless transmissions of confidential data whether printed or copied, can be intercepted and hard drives containing confidential information can be accessed. Devices with wireless capabilities should follow the same security rules as other wireless devices (see “4.2 Wireless Network Communications”). Devices with non-volatile memory should have their memories cleared on a regular basis.
15. Sites using the District’s Simple Mail Transfer Protocol (SMTP) relay server must use it for the purpose explicitly listed when requesting approval. The IP address will be monitored and if use that is inappropriate or inconsistent with the requested access of the gateway is found to occur, ITS reserves the right to revoke this access.

4.1.3 Downloads and Internet

1. Games, chat sessions, peer-to-peer (P2P), and instant messenger applications are prohibited on the M-DCPS network unless there is a legitimate educational purpose and prior approval. These applications

bypass network security such as anti-virus scans and therefore are a risk. Chat and instant messenger applications can tie up a great deal of bandwidth and may be used by students for many illicit purposes. In particular, students can easily be put in contact with persons who may be a threat to their safety. In cases where there is chat capability within a software package for vendor support purposes, users should only use this to work with support for the application.

2. MPEG files (including the MP3 and MP4 formats) are audio and video files digitized and/or compressed into a format that can be read and transferred by a computer. Downloading or storing files of these or any other formats that do not have any educational value is prohibited. These files, though greatly compressed, are still fairly large and can tie up a great deal of bandwidth and computer storage. In addition, most have been illegally copied and infringe on copyrights owned by the artists and record/movie companies (refer to section 4.1.1 Network Structure, Hierarchy and Requirements, number 6, especially Copyrights). Users should be aware that record/movie companies are notifying the District when an MPEG file of copyrighted material has been downloaded and what location received it.
3. Streaming audio and video is basically the same type of data as MPEG but it is being sent in a continuous stream directly to the computer's media player rather than as a file for storage. This sort of streaming content uses large amounts of District bandwidth and, like the mpeg files mentioned above, may involve copyright infringement. For these reasons, streaming audio and video is also prohibited unless it has a valid educational purpose and site supervisor approval.
4. Skype and other Voice over IP (VoIP) applications are prohibited without a valid educational purpose and authorization. These applications consume large amounts of bandwidth and require client software that can introduce security vulnerabilities unless they are updated on a regular basis.
5. Applications such as WebWhacker that allow a user to download all of the content from a Web page automatically, in large bursts, and without user intervention, are prohibited unless there is a valid District purpose, as they consume large amounts of bandwidth.
6. "Hacking software" has been designed to allow unauthorized persons to infiltrate computers on the network, view and modify data, spy on a user's keystrokes in an effort to get user-ids and passwords. ITS reserves the right to randomly scan or monitor any computers attached to the M-DCPS network in an effort to detect the presence of any "hacking software" or irregular operations that may be present on the network. ITS also reserves the right to disconnect any device or user on the network that appears to pose a threat.

   Regarding the use of network administration software, users should be aware of the following:

a. Improper use of scanning tools can corrupt system files, user account information, and databases.

b. Hackers generally start their illicit activities by scanning networks searching for unprotected resources with these tools.

c. Any scan of the M-DCPS network may appear to be the work of a malicious entity.

d. Scanning anywhere in the M-DCPS WAN is traceable to the source and those responsible can be identified.

Local Network Administrators may scan their own network within the framework of their assigned and authorized duties. Requests to scan the local network by persons who are not members of the site staff (whether it is a school or an administrative department) require approval from ITS. Under no circumstances will scanning outside the local network site, either of another LAN in M-DCPS or public or private networks outside M-DCPS, be permitted. All applicable local, state and federal regulations apply. It should be noted that, in the case of scanning networks outside M-DCPS, local and federal law enforcement officials are unable to tell the intention of illicit scanning and are therefore vigorously prosecuting all instances. This prosecution is generally independent of M-DCPS disciplinary activities.

7. "Cracked software" is software that has had its internal security broken (cracked) and has been made available to others. Cracked software is strictly prohibited.

8. M-DCPS Internet content filtering technology limits the kinds of Internet sites that can be viewed on the M-DCPS Internet connection. Pornography sites, sites advocating violence or bigotry, sites with games, hacking tools, and cracked software are examples of what will be blocked. There will be no bypassing of the M-DCPS Internet content filtering without ITS authorization. Software that bypasses filtering and other data security mechanisms includes AOL full-client and other Internet Service Provider (ISP) full-client applications. Installation of this software on District computers is prohibited without authorization. Internet content filtering audit logs showing Internet activity and sites visited by users may be reviewed at any time.

9. Network file shares should not be used for storing personal pictures and videos, and music files and M-DCPS will not be liable for any lost personal files.

4.1.4 Authorizations and Access

1. Certain applications are particularly sensitive and supervisors must be careful to adhere to District mandates regarding numbers of staff given authorization to update these applications. These mandates are

issued by School Operations. The following is a list of applications that fall into this category:

a. Mainframe academic grade update

b. Grade Book Manager and Attendance functions

c. Payroll data entry and approval

2. Site supervisors are reminded that staff authorizations are listed in the "Authorizations for Employees by Location" report (Product number T0802E0101) available through the Cntl-D Web Viewer on the Intranet. This report is now run monthly and has been expanded to include listings for each of the specific sensitive areas listed in number 1 above.

4.1.5 E-Mail

Users are reminded that the District Staff E-Mail Policy (See section 4.1.1 Network Structure, Hierarchy, and Requirements, number 6) requires individual users to keep all e-mail that is required to be kept by federal, state, and local statute. Accessing other users' e-mail without authorization or valid District purpose is prohibited. The e-mail system is an application containing potentially sensitive information and users should take all precautions to protect it, including locking their computer and protecting their passwords as outlined elsewhere in this document.

ITS runs regularly scheduled e-mail backups that are intended to be used only for system recovery. They are not for archival purposes. These backups are kept for at least 10 days but no more than 3 weeks and are then deleted

4.2 Wireless Network Connections

Wireless network components have become a very attractive alternative to cabling due to their low cost and relative ease of installation. If installed without proper security, however, they pose the same threat to our informational assets as if a hacker were able to plug directly into one of our network jacks. Users should observe the following:

1. Network installations with wireless components must maintain the highest level of security available. Older M-DCPS wireless installations should be updated with any vendor patches supplying improved security features. If the device has no security available, it must be replaced immediately. New installations should use only products with high-level encryption. In all cases, the installation's security features must be turned on.

2. ITS must be informed of all District wireless installations. This includes school sites.

3. All wireless installations must be "enterprise capable". This allows configuration and management to be handled remotely. A low cost, residential-type Access Point (AP) is not enterprise capable. In addition, all wireless installations must include surge protectors, with battery backups

recommended. Experience has shown that security settings on wireless devices have been reset by lightening strikes or power surges. This means the security may have been turned off without the knowledge of staff.

4. Site supervisors and technicians should check that other staff does not install rogue devices without approval and/or correct security settings. These devices become open doors to hackers seeking to get into the network.

5. Municipalities, houses and businesses around a site may provide accidental associations with their networks. Care should be taken to avoid tapping into outside wireless networks.

6. If adequate security cannot be achieved within the boundaries of the manufacturers' built-in security mechanisms, a firewall should be placed between the workstations and the Access Point (AP) in such a way that the transmissions have a high level of encryption (3DES, also known as Triple-DES, if possible).

7. When utilizing any outside wireless network or wireless service, Virtual Private Network (VPN) technology should be used.

8. New wireless installations in the ITS/SBAB core network must first be approved by ITS network administration staff. Information regarding the purpose and certification that the installation incorporates the highest level of security possible must be provided.

9. ITS is authorized to randomly scan or monitor for the presence of unauthorized or insecure wireless devices connected to M-DCPS networks. ITS also reserves the right to disconnect any wireless device that appears to pose a threat to an M-DCPS network. District staff should be aware that because unsecured wireless devices are such a serious security concern, instances of non-compliance with these standards will be reported and unauthorized devices confiscated.

10. Staff should always consider purchases of wireless devices through the M-DCPS bid process first. Devices purchased through the bid are enterprise capable, have more "industrial strength," and include surge protectors, installation, and support. Additionally, in some cases they are "e-Ratable" and so the cost to the school may be about the same as the low-end devices purchased outside the bid. Check with an e-Rate expert for details.

11. Because there is such a wide range of wireless devices, it is not possible to list all possible security options. However, at the very least, the following options should be set:

    - the broadcast option should be turned off,
    - encryption should be turned on,
    - membership should be limited to those machines having id's defined as being authorized to join the network and having the correct network name,
    - all default passwords should be changed.

For more details, see the M-DCPS Wireless Security Tech Note at:
http://pdfs.dadeschools.net/techsupport/datasecurity/wireless_security.pdf

4.3 Portable Devices

Use of laptop/notebook computers and Personal Digital Assistants (PDAs) has become more and more common in the District. Most now have network and wireless connectivity, video and voice functions, and significantly more powerful computing and storage capabilities. As with any components of the M-DCPS computer system, all security precautions must be taken to ensure that the informational assets of the District are not put at risk.

Portable devices require extra attention because physical security for these devices is much more difficult to achieve. Users must be aware of the ease with which laptops and especially PDAs can fall into the wrong hands due to their small size and portability, and the resulting loss of security. Among the issues to consider are:

1. Wireless portable devices must have the same kinds of security discussed in section 4.2 Wireless Network Connections. Encryption must be set at a level that ensures network security and should be of a type that changes keys frequently.
2. Use of power-up and activity-timer passwords is required on PDAs and notebooks.
3. All portable devices, including PDAs, are susceptible to viruses and therefore should have anti-virus software installed. It should be set to scan e-mails and attachments as well as regular files if available. Timely installation of patches to the Operating System (OS) will help ensure that the vulnerabilities exploited by viruses and Trojans are eliminated as the vendor uncovers and patches them.
4. Confidential data kept on any laptop or other portable device must be encrypted in the event the device is lost or stolen. Encryption of this nature can be provided as part of the hardware, part of the OS, or a third-party application and may be file-specific, folder-specific or whole-disk. Note that some versions of Windows Vista, 3rd-party vendors and hard-drive manufacturers now provide these capabilities. Confidential M-DCPS data should be set to “private” and “hidden” on Palm or similar attributes while stored on another PDA. It can also be locked by 3rd-party software. This includes sensitive memoranda, student or staff data, lists of passwords, home addresses and phone numbers of exempt staff, social security numbers, and credit card account information. Applications on these devices should have any available security features turned on.
5. Communications with the network via the Internet or Intranet must be secure and require a valid network id and password.

6. Network passwords are not to be saved on the device; they must be retyped with each network logon. Passwords should never be written or otherwise stored on the device itself or the carrying case.
7. If tokens (hardware or software) are utilized, the token should be carried separately from the device.
8. Mobile devices should never be left unsupervised in a location with public access.
9. Contact information should be provided at the log-in prompt so that a lost device may be returned if found.
10. Forgotten PDA passwords will require the user do a Hot Synch and a hard reset, which will cause all data entered since the last Hot Synch to be lost. Users should therefore run Hot Synchs on a regular basis as a form of backup. If possible, the District should standardize on a synching product.
11. PDAs that are used for M-DCPS business should be synched to the server if possible rather than the desktop to make sure the data is more secure and available to others in the department authorized to access it.
12. BlackBerry users should note the following:
    a. Passwords can be reset from ITS by notifying the ITS Systems Support Help Desk at 305-995-3705.
    b. If the device is lost or stolen, it should be reported immediately to the Help Desk at 305-995-3705. Steps can be taken by ITS to lock the device down and/or wipe the data on the device. If the device is found or returned, ITS can also restore the data once notified.
    c. Administrative applications available on the BlackBerry still require the use of the appropriate network and mainframe passwords.
13. Data on damaged PDAs should always be cleaned if at all possible before the device is sent to a repair facility or disposed of.
14. Bluetooth devices connected to PDAs and cell phones should have built-in security turned on as nearby Bluetooth devices may pick up their signals.
15. Apple iPhones must have firmware version 2.0 or higher to connect to the network and users must turn on the “Ask to Join Networks" setting, use VPN for any outside connection used, and set a pass code.

5.0 Staff Security Responsibilities

All M-DCPS authorized staff have the following security responsibilities:

1. All authorized staff is responsible for protection of M-DCPS assets, including computers and data.
2. Users are prohibited from using M-DCPS data, applications, software, equipment, listings, or any other District computer assets without authorization. Access must be in support of District goals, job requirements,

or instructional activities, and can not be used to improperly view or remove confidential data, misuse or incapacitate equipment or applications, or interfere with or deny service to others.

3. M-DCPS computer equipment is for M-DCPS business and educational functions only. It is not to be used for unauthorized activities.

4. Authorized staff will not use or reveal data except in an official M-DCPS need-to-know capacity. This includes, but is not limited to, data that appears in downloads, on reports or terminal screens, on desktops, in recycle folders or application caches, or any other methods used to store, display or communicate the data. They must see to it that students or other unauthorized persons never have unsupervised physical or virtual access to administrative computers anywhere at their location. This also applies to descriptions and/or diagrams of M-DCPS network infrastructure and security audit findings. This information can be used by hackers seeking to gain illicit entry into the network and the more people who have this information the greater the chance of exposure to persons with bad intentions.

5. M-DCPS authorized staff must not install any hardware or software that compromises data, passwords, applications, or any other computer-related M-DCPS asset unless authorized to do so by ITS. Staff should also be careful not to expose sensitive data using the file-sharing capabilities of their computer.

6. Unlicensed copies of software are not to be created, installed or used. Personally owned licensed software must be approved by local administration before being installed on M-DCPS equipment. The software must have legitimate business or instructional functions. Proof of licensing must be presented to the local administrator and should be kept on file at the site along with the licenses of District-owned software installed.

7. Authorized staff is not to engage in any activities that might compromise computer assets, including passwords. This also includes using M-DCPS computer assets to access and inappropriately use networks outside of M-DCPS.

8. Security software (anti-virus programs, patch management software, spyware, and hacking software detectors, domain and local computer policy) should be loaded and running on all computers sharing files over the network. This software is required to be on all servers and must be updated regularly. The anti-virus software should be set-up to check e-mail attachments. Regular updates of the protection software should also be made available to the other computers in the domain and installed in the most expedient manner possible. Staff members who use outside providers, such as AOL or Hotmail, for their e-mail services must also load and maintain current versions of anti-virus software with settings to check e-mail attachments. This is due to the threat to M-DCPS network resources from malicious programs sent by hackers via attachments in e-mail.

9. Vendors or other outside agencies seeking access to M-DCPS equipment or data are to be informed of these Standards and ITS network

administrators should be notified. The vendor's equipment will not be migrated to the dadeschools network unless it is determined by ITS that this can be done. Locations should reserve some static TCP/IP addresses for situations where a vendor (such as a clinic providing services to the location's students) needs access to connect to their own company's systems. This would allow ITS to provide content filter bypass and/or a Virtual Private Server (VPS), as necessary.

10. The specific functions for which users are to be authorized are determined and/or approved by the site supervisor or designee. Any modification of authorizations without the approval of the supervisor or designee is prohibited.
11. Site supervisors are responsible for ensuring that all policies are observed.
12. Site supervisors are also responsible for informing authorized staff and users of these policies and staff security responsibilities. In addition, site supervisors are required to review and retain a signed copy of the most recent RACF report showing that the authorizations held by site staff are appropriate, especially in regard to high risk authorizations like grade change (See section 4.1.4 Authorizations and Access).
13. Authorized staff should be informed of M-DCPS computer security standards. New or recently authorized staff should be informed during orientation. Use of M-DCPS equipment and/or networks constitutes acceptance of these policies.
14. Any authorized staff approached with a proposition to violate these Standards should notify his/her supervisor and/or ITS. This also applies to any authorized staff observing any activity that may be a violation of these Standards.
15. Users are only allowed to view and/or use those applications for which they have been authorized by their supervisor or other M-DCPS-designated authorizing staff.
16. All software should be updated with patches and service packs provided by the manufacturer as they become available, especially if there is a security enhancement. Users should be aware that although these updates are occasionally released before all the bugs have been detected and removed, and it is preferable to do research and/or testing before applying the patch to production systems, too often the patch must be applied as soon as possible because of the critical nature of the update.
17. District-wide initiatives such as loading anti-virus software, patch management software, user registration in the P-Synch password reset application, spyware detection/removal software, Intrusion Prevention Systems (IPS), power management, wireless WAN management, and migration to the dadeschools domain must be complied with. Future District-wide initiatives may include desktop management. In addition, all computers must be named according to the M-DCPS naming convention, which requires the location number be the first four digits of the name.

Computers which do not comply with the District initiatives may be excluded from network and Internet access until the security standards are met.

18. Users should never load software or register at a Web site using District computers without carefully reading the privacy policy and End User License Agreement (EULA) first. Free software, in particular, often comes with the understanding that spyware and/or adware will be loaded on your machine. This kind of software runs in the background and allows others to watch what you do on your computer, and loads ads, software and updates on your computer without your knowledge. Applications like Hotbar and peer-to-peer (P2P) music sharing applications like Kazaa are infamous for doing this. Spyware and adware can also be loaded on your machine when you visit some web sites. Be sure that your browser preferences are set so that software cannot be loaded on your computer without notifying you. Anti-spyware software is available that searches for known spy ware/ad-ware and cleans it from the machine.
19. Stolen computer equipment must be reported to the site supervisor and network administrator immediately so that steps can be taken to protect the network from unauthorized access.
20. It is the responsibility of all staff to protect our students from inappropriate material, especially on the Internet. The M-DCPS Internet Acceptable Use Policy delineates the proper use of the Internet by students and staff and defines that material which is offensive, obscene or otherwise inappropriate. The District must also protect itself from misuse of its network assets (for example, copyright infringement, over-consumption of bandwidth via streaming audio or video). The Internet Content Filtering application may be of use in these cases.

    Staff who discover students accessing inappropriate sites should report the student to the Principal and these sites to ITS. If possible, ITS will use the District's Internet Content Filtering mechanism to block this sort of inappropriate material or use. The District reserves the right to assign staff to evaluate reported inappropriate sites and block them if they are determined to be offensive or in some way a misuse of District networks. ITS staff performing this function will maintain a folder with these requests.

Acceptance of employment or contracts with M-DCPS will signify acceptance of these standards by the user. Failure to comply with this or any M-DCPS computer security policy or standard may result in termination of employment, termination of contract, and/or prosecution.

5.1 User-ids and Passwords

Regarding user-ids and passwords:

1. No one is permitted to access M-DCPS networked computers without a user-id and password.
2. M-DCPS will provide user-ids only with the approval of the staff member's supervisor.

3. Users are responsible for all activity associated with their user-id. When a user is finished using a computer or will be leaving the computer unattended, they must log off or lock the computer (CTRL-ALT-DELETE, Lock Computer) to prevent their account from being compromised.
4. User-ids will be revoked when an incorrect password has been entered an appropriate number of times within an appropriate period.
5. User-ids will be revoked on all computer platforms when the user is terminated or transferred.
6. User-ids may be revoked, cancelled, or suspended at any time.
7. A user-id may, at the ITS Data Security Department supervisor's discretion, be revoked or cancelled if it has not been used for 100 days or more.
8. Network user-ids will consist of the 6-character employee number. This allows administrators to locate and revoke all M-DCPS user-ids if the employee is accessing data illegally or has been terminated.
9. Passwords will be 8 characters long, including at least 1 numeric character.
10. Passwords must be changed every 180 days, unless the user has access to certain types of sensitive data as determined by Senior Staff, in which case the password must be changed every 30 days; or the account is a system or FTP account, in which case senior staff may decide if and when the password should be changed. Notification of an impending password change deadline will be provided whenever possible.
11. Users are restricted from reusing their last 6 passwords.
12. Users are requested to refrain from using common passwords (i.e., first name, last name, spouse or pet names, school nicknames, the word "password," "123456," "ABCDEF,"). Persons seeking unauthorized access easily guess these. There is also password-guessing software that can try thousands of common words and names used as passwords in seconds.
13. Users may change their password at any time.
14. If users suspect the confidentiality of their password has been compromised, they must change their password immediately. If they are unable to change the password themselves, they should contact their supervisor or appropriate staff at ITS to have the reset performed.
15. Staff must not engage in any activity that may reveal or otherwise compromise their own or another user's password.
16. There is to be no auto-caching of passwords. This means that the password is to be retyped each time the user logs in to the network or application.
17. The administrator of the network/application should always disable "Guest" default accounts. In addition, the administrator should immediately change all generic and default system passwords such as "administrator" and "password." This user-id and password should be stored in a secure location and only used in an emergency. All individuals should be assigned specific rights to allow an audit trail of the work performed, e.g., the network administrator has an id that has administrator rights. The audit trails should be reviewed by management to ensure that only approved authorized changes have been made.
18. Under no circumstances should any individual, including supervisors, ask for any other individual's network password or RACF password.

19. Avoid transmitting or storing passwords in clear text whenever possible. If available, password encryption should be turned on.
20. Local Windows passwords are not secure and thus only the network log-on should be used for security and authentication.
21. In the interest of personal security, users should be aware that in the future, their network password will control access to their personal information in the Human Resources (HR) system and so should use even more care to protect the integrity of their password.

6.0 Changes to Standards

ITS is responsible for periodically reviewing these standards to ensure that the data is provided adequate protection. This is especially true in the rapidly changing world of computer and related equipment, networks, Internet, software, databases and data access techniques. It is incumbent on all M-DCPS departments involved in data processing and security to keep abreast of the latest changes in these areas.

6.1 Data Security Services

Requests for security services can be made through the ITS Help Desk. Extra information may be required from the user and a form may have to be filled out. Users should provide contact information and an e-mail in case extra information is necessary. The e-mail should be sent by the site supervisor and as such will be viewed as an officially signed document.

Glossary

1. IBM OS/390 Security Server, also known as Resource Access Control Facility (RACF) - IBM mainframe security software introduced in 1976 that verifies user-ID and password and controls access to authorized files and resources.
2. Local Area Network (LAN) - A communications network that serves users within a confined geographical area. It is made up of servers, workstations, a network operating system and a communications link.
3. Wide Area Network (WAN) - A communications network that covers a wide geographic area, such as state or country.
4. Transmission Control Protocol/Internet Protocol (TCP/IP) - A communications protocol developed under contract from the U.S. Department of Defense to inter-network dissimilar systems. It is a de facto UNIX standard, but is now supported on almost all platforms. TCP/IP is the protocol of the Internet.
5. File Transfer Protocol/File Transfer Program (FTP) - In a TCP/IP network (Internet), a set of commands used to log onto the network, list directories and copy files. It may also refer to a computer system on the Internet that maintains files for downloading.

Index