MEMORANDUM April 01, 2002

TO: Superintendent's Direct Reports
All School Principals
All Non-School Site Administrators

FROM: Ralph G Lewis, Executive Assistant
Strategic Initiatives

SUBJECT: MIAMI-DADE COUNTY PUBLIC SCHOOLS NETWORK SECURITY POLICY REVISION

In February 2001, Miami-Dade County Public Schools (MDCPS) implemented its first Network Security Policy. Dealing as it does with technology issues, this document will require revisions to incorporate the latest developments in this tremendously dynamic arena and how they affect the district.

This year alone, some different technologies have become commonplace in the district and some of the original policy statements required clarification. Among the new issues addressed in this revision are:

- Security for Wireless connections to the LAN and concerns that the network is not compromised.
- Portable computing devices such as laptop/notebook computers and Personal Digital Assistants (PDAs) and the procedures necessary to protect them from loss or theft .
- Downloading of MP3 files is prohibited except for valid, purely educational purposes.
- Application software security features must be activated when the application involves confidential information.
- How users should deal with the possibility that their password has been compromised.

This document has been reviewed by representatives from Instructional Technology and Media Support, Office of Management and Compliance Audits and Office of Information Technology.

After reading the policy, please complete a brief online survey to assist the district in strengthening and maintaining Network Security. You may wish to complete the survey with your computer technician present to clarify the technical issues as they apply to your location. The survey can be found at: **http://surveys.dadeschools.net**

Your full compliance is required to keep our networks secure. Training is available at OIT. Clarification or assistance is available from System User Support, Office of Information Technology, at 995-3705.

Attachment

cc: Superintendent's Executive Staff

NETWORK SECURITY POLICY - ADMINISTRATIVE SUMMARY

1.0 Overview

Miami-Dade County Public Schools (MDCPS) 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. MDCPS 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 is not compromised.

1.1 Objectives

MDCPS realizes that information is a valuable asset and must be protected from loss, theft, and unauthorized modification and disclosure. All security measures must conform to established MDCPS policies and applicable federal, state, and local laws.

1.2 Risks to MDCPS

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 MDCPS data. The technical risks include:

- Altered data
- Stolen and intercepted data
- Data rendered inaccurately
- Destroyed data
- Loss of MDCPS' ability to process data.

Business risks to MDCPS include:

- Lawsuits for not protecting sensitive data
- Loss of funding (for example, FTE) due to transmission of incorrect data to other agencies
- Unfair penalty or advantage to students due to 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 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 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), MDCPS board rules, and decisions by senior staff and/or the data owners (see section 5.2 of this document).

1.3 Background of MDCPS Data Security

Historically almost all MDCPS data was kept on the MDCPS mainframe at the Office of Information Technology (OIT) 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 would 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 MDCPS employees, consultants, vendors, auditors, students, temporary help and others authorized by MDCPS to use the specific MDCPS computer systems, applications and information required for the performance of their job or function.

The Network Security policy applies to:

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

All MDCPS staff and authorized non-staff must be aware of the risks and act in the best interest of MDCPS. This policy statement details staff's responsibilities for computer security. Unauthorized persons who attempt to use MDCPS computer resources will be prosecuted to the fullest extent possible.

3.0 Physical Security

Adequate building security (both physical and environmental) must be provided for the protection of all physical and logical MDCPS 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 MDCPS Network Systems Security

Network systems include any local area network (LANs)[2], wide-area networks (WANs)[3], dial-up, Internet, servers, server connections, hubs, routers, lines, software, and data that are outside the MDCPS mainframe system. The security must include both physical and logical layers of protection. As MDCPS moves from storing and transferring sensitive information used within the MDCPS 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.

- As a statement of direction, all administrative PC-type servers in MDCPS should migrate to the Windows 2000 (or above) operating system. Users of servers currently using Windows NT, Novell, or any other PC network operating system should strongly consider migrating to Windows 2000 when the server is ready for its next upgrade.
- Windows 2000 employs Active Directory Services (ADS), a hierarchical process similar to a pyramid. OIT will establish and maintain the Windows 2000 root ADS (the top of the pyramid) for MDCPS and determine local and group policy settings. All other district servers will be added to the OIT established Active Directory structure as they come online or upgrade to Windows 2000.
- Below the root on the pyramid are local domains. Local domains are simply smaller networks with their own server that connect to the MDCPS network. These include networks at a school or administrative site. Local domain administrators must not change local policies from MDCPS standards or override MDCPS group policy. Domain administrators must also strictly limit access to their domain from other domains. OIT must be given Enterprise Administrator rights to all domains attached to the MDCPS network. OIT must provide notification of group policy changes.
- Firewalls are servers that function as a barrier preventing unauthorized outside access to the MDCPS network. Exceptions requiring access from the outside must be documented by filling out OIT's *Remote Client Support Agreement IP Entry (FM-6045).* OIT will keep firewall audit logs and review them daily for illicit activity against the firewall.
- Access to secure mainframe applications via the network requires RACF authorization.

- Dial-in to the MDCPS network requires network authorization and access authentication.
- As spelled out in a memo from the Superintendent dated 11/09/1999, games, chat sessions and instant messenger applications are prohibited on the MDCPS network.
- MDCPS "Acceptable Use" policy regarding use of the Internet must be read and followed at all times by all MDCPS users. This document is available on the Internet at http://www.dade.k12.fl.us/aup/.
- Downloading MP3 files (audio files digitized and compressed into a format that can be read and transferred by a computer) that do not have any educational value is prohibited. MP3 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 companies (refer to School Board Rule 6GX13-4C-1.063). Users should be aware that record companies are notifying the district when an MP3 file of a copyrighted piece has been downloaded and what location received it.
- Each department or school must maintain a disaster contingency plan to provide for recovery of data in case of catastrophic loss. At minimum, all MDCPS 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.
- The use of remote access services (RAS) such as DSL, dial-in technology with a modem, etc., is prohibited unless authorized by OIT. This provides a "back door " around network security by providing users a direct connection to a remote server.
- The use of communications software that provides the ability to remotely "take over" a network connected PC is prohibited unless authorized by OIT.
- "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, etc. OIT reserves the right to randomly scan or monitor any computers attached to the MDCPS network in an effort to detect the presence of any "hacking software" or irregular operations that may be present on the network. OIT also reserves the right to disconnect any device or user on the network that appears to pose a threat.
- "Cracked software" is software that has had its internal security broken (cracked) and has been made available free to others. Cracked software is strictly prohibited.
- MDCPS Internet content filtering technology limits the kinds of Internet sites that can be viewed on the MDCPS 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 MDCPS Internet content filtering without OIT authorization. Internet content filtering audit logs showing Internet activity and sites visited by users will be reviewed on a regular basis.
- Administrative computers are defined as non-classroom computers on which MDCPS requisition and business functions, 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.

- 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, possible storage of grade and test data on removable media, and limiting unsupervised student access as much as possible.
- All administrative computers and server consoles that are used to access or control sensitive data should have a screen saver timeout and password after a specific period of inactivity to prevent unauthorized persons from accessing these environments. These computers may have boot up passwords.
- 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.
- Outside access to MDCPS 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 MDCPS network.
- 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.
- 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 OIT.
- 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 5.3 "Non-mainframe System Security."
- 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.

4.1 Wireless Network Connections

Network installations with wireless components must maintain the highest level of security available. Older MDCPS wireless installations should be updated with any vendor patches supplying improved security features. New installations should use only products with high-level encryption. In all cases, the installation's security features must be turned on.

4.2 Portable Devices

Use of laptop/notebook computers and Personal Digital Assistants (PDAs) has become more and more common in the district. Many now have network and wireless connectivity and in the near future there will be video and voice functions as well as significantly more powerful computing and storage capabilities. As with any components of the MDCPS 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:

- Wireless portable devices must have the same kinds of security discussed in section 4.1. Encryption must be set at a level that ensures network security and should be of a type that changes keys frequently.
- Use of power-up passwords is required on PDA’s and notebooks.
- All portable devices, including PDA’s, 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.
- Confidential MDCPS data should be set to “private” and “hidden” on Palms or similar attributes while stored on another PDA. It can also be locked by third-party software. This includes sensitive memos, student data, lists of passwords, home addresses and phone numbers of exempt staff, credit card numbers, etc.
- Communications with the network via the Internet or Intranet must be secure and require a valid network id and password.
- Network passwords are not to be saved on the device, but must be retyped with each network logon. Passwords should never be written or otherwise stored on the device itself or the carrying case.
- If tokens (hardware or software) are utilized, the token should be carried separately from the device.
- Mobile devices should never be left unsupervised in a location with public access.
- Contact information should be provided at the login prompt so that a lost device may be returned if found.
- 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.
- PDA’s that are used for MDCPS 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.

5.0 Staff Security Responsibilities

MDCPS authorized staff have the following security responsibilities:

- All authorized staff is responsible for protection of MDCPS assets, including computers and data.

- MDCPS computer equipment is for MDCPS business and educational functions only. It is not to be used for unauthorized activities.
- Authorized staff will not use or reveal data except in an official MDCPS need-to-know capacity. This includes, but is not limited to data that appears in downloads, on reports or terminal screens, or any other methods used to display or communicate the data. They must see to it that students or other unauthorized persons never have physical or virtual access to administrative computers anywhere at their location.
- MDCPS authorized staff must not install any hardware or software that compromises data, passwords, applications, or any other computer-related MDCPS asset unless authorized to do so by OIT. Staff should also be careful not to expose sensitive data using the file-sharing capabilities of their computer.
- Unlicensed copies of software are not to be used or created except as backup.
- Authorized staff is not to engage in any activities that might compromise computer assets, including passwords. This also includes using MDCPS computer assets to access and inappropriately use networks outside of MDCPS.
- Security software (anti-virus programs, Back Orifice detectors, computer policy, etc.) 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 MDCPS network resources from malicious programs sent by hackers via attachments in e-mail.
- Vendors or other outside agencies seeking access to MDCPS equipment or data are to be informed of this policy and OIT network administrators should be notified.
- Site supervisors are responsible for ensuring that all policies are observed.
- Site supervisors are also responsible for informing authorized staff and users of these policies and staff security responsibilities.
- Authorized staff should be informed of MDCPS computer security policy. New or recently authorized staff should be informed during orientation. Use of MDCPS equipment and/or networks constitutes acceptance of these policies.
- Any authorized staff approached with a proposition to violate this policy should notify their supervisor and/or OIT. This also applies to any authorized staff observing any activity that may be a violation of this policy.
- Users are only allowed to view and/or use those applications for which they have been authorized by their supervisor or other MDCPS-designated authorizing staff.
- All software should be updated with service packs provided by the manufacturer as they become available, especially if there is a security enhancement.

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

5.1 User-ids and Passwords

Regarding user-ids and passwords:

- No one is permitted to access MDCPS networked computers without a user-id and password
- MDCPS will provide user-ids only with the approval of the staff member's supervisor.
- Users are responsible for all activity associated with their user-id
- User-ids will be revoked when an incorrect password has been entered 3 times in a row within a 30-minute period.
- User-ids will be revoked on all computer platforms when the user is terminated or transferred.
- User-ids may be revoked, cancelled, or suspended at any time.
- A User-id may, at the OIT Data Security Department supervisor's discretion, be revoked or cancelled if it has not been used for 100 days or more.
- Network user ids will consist of the 6-character employee number. This allows administrators to locate and revoke all MDCPS user ids if the employee is accessing data illegally or has been terminated.
- Passwords will be 6 – 8 characters long, including at least 1 numeric character.
- Passwords must be changed every 90 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. Notification of an impending password change deadline will be provided whenever possible.
- Users are restricted from reusing their last 6 passwords.
- 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", etc.). 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.
- Users may change their password at any time.
- 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 OIT to have the reset performed.
- Staff must not engage in any activity that may reveal or otherwise compromise their own or another user's password.
- 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.
- The administrator of the network/application should immediately change all generic system passwords such as "Administrator". 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 only approved authorized changes have been made.

- Under no circumstances should any individual, including supervisors, ask for any other individual's network password or RACF password.
- Avoid transmitting or storing passwords in clear text whenever possible. If available, password encryption should be turned on.
- Local Windows passwords are not secure and thus only the network logon should be used for security and authentication.

5.2 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 that 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.

5.3 Non-Mainframe System Security

Non-Mainframe systems (LAN and WAN) must have the same protection methodology in place as do mainframes to ensure MDCPS 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, databases, etc. "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:

- Auditing/logging of such security-relevant information as logon and resource access violations
- Security modifications and system administrator events
- Ability to audit /log specific users and resources on demand
- Ability to send specific security sensitive events directly to a specified administrator's workstation, terminal, or e-mail, preferably with an audible alarm

6.0 Changes To Policy

The OIT Data Security Department, in conjunction with other OIT departments (Network & Internet Services, Technical Support, Systems and Programming, etc.) is responsible for periodically reviewing this policy 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 MDCPS departments involved in data processing and security to keep abreast of the latest changes in these areas.

6.1 Data Security Department Services

Requests for services from the OIT Data Security Department can be sent via e-mail to any of the members of the department and will be processed accordingly. Extra information may be required from the user and a form may have to be filled out. Users should provide contact information in the e-mail in case extra information is necessary.

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. A computer system on the Internet that maintains files for downloading.