

NETWORK SECURITY STANDARDS - 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

MDCPS NETWORK SECURITY STANDARDS

- 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 Information Technology Services (ITS) and access was strictly controlled through the use of the mainframe IBM OS/390 Security Server¹ (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. These specific functions are determined and/or approved by the site supervisor. Modification of authorizations without the site administrator's approval is prohibited.

The Network Security Standards apply to:

- All authorized staff, volunteers, students and vendors 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. These standards detail 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 (LAN)², wide-area network (WAN)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 network⁴, employees must pay particular attention to the security of these assets.

1. 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. Desktops should similarly be migrated to Windows 2000 or above when possible to take advantage of higher levels of security.
2. Windows 2000 employs Active Directory Services (ADS), a hierarchical process similar to a pyramid. ITS 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 ITS established Active Directory structure as they come online or upgrade to Windows 2000.
3. 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 policies or override MDCPS group policy. Domain administrators must also strictly limit access to their domain from other domains. ITS must be given Enterprise Administrator rights to all domains attached to the MDCPS network. ITS must provide advanced notification of group policy changes.
4. 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 ITS's *Remote Client Support Agreement IP Entry (FM-6045)* (old), or either of the new *VPN Access Request* forms (FM-6629, for vendors or employees). ITS will keep firewall audit logs and review them daily for illicit activity against the firewall.

MDCPS NETWORK SECURITY STANDARDS

5. Access to secure mainframe applications via the network requires RACF authorization.
6. Dial-in to the MDCPS network requires network authorization and access authentication.
7. Games, chat sessions and instant messenger applications are prohibited on the MDCPS network unless there is a legitimate educational purpose and prior approval. 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.
8. MDCPS Board rules/directives/standards regarding the following topics must be read and followed at all times:

MDCPS "Internet Acceptable Use" policy:

<http://www.dadeschools.net/board/rules/Chapt6/6A-1.112.pdf>

MDCPS Board Rule regarding Copyright:

<http://www.dadeschools.net/board/rules/Chapt4/4C-1.06.pdf>
<http://www.dadeschools.net/board/rules/Chapt4/4C-1.061.pdf>
<http://www.dadeschools.net/board/rules/Chapt4/4C-1.062.pdf>
<http://www.dadeschools.net/board/rules/Chapt4/4C-1.063.pdf>

MDCPS Superintendent's E-Mail Directive and memo:

http://techsupport.dadeschools.net/data_security/MDCPS%20E-mail%20Policy.pdf

http://techsupport.dadeschools.net/data_security/E-mail%20Policy%20Cover%20Memo.pdf

(At this writing (05/2004) a draft Board Rule covering MDCPS e-mail policy has been created. When this document becomes Board rule it will supercede the above directive).

9. 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 8 above). 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.

Streaming audio and video is basically the same type of data 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

MDCPS NETWORK SECURITY STANDARDS

- prohibited unless it has a valid educational purpose and site supervisor approval.
10. 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.
 11. The use of remote access services (RAS) such as Digital Subscriber Line (DSL), dial-in technology with a modem, etc., 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.
 12. 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.
 13. "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. ITS 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. ITS also reserves the right to disconnect any device or user on the network that appears to pose a threat.

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

1. Improper use of scanning tools can corrupt system files, user account information and databases.
2. Hackers generally start their illicit activities by scanning networks searching for unprotected resources with these tools.
3. Any scan of the MDCPS network may appear to be the work of a malicious entity.
4. Scanning anywhere in the MDCPS 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 either the Network Services or Data Security groups of ITS. Under no circumstances will scanning outside the local network site, either of another LAN in MDCPS or public or private networks outside MDCPS, be permitted. All applicable

MDCPS NETWORK SECURITY STANDARDS

- local, state and federal regulations apply. It should be noted that, in the case of scanning networks outside MDCPS, 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 MDCPS disciplinary activities.
14. "Cracked software" is software that has had its internal security broken (cracked) and has been made available to others. Cracked software is strictly prohibited.
 15. 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 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.
 16. 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.
 17. 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, installing software and operating system patches as necessary, (especially critical security patches), 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, etc.) should be separate from teacher accounts.
 18. 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 or some other lockout mechanism to prevent unauthorized persons from accessing these environments. These computers may also have boot up passwords.
 19. 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.
 20. 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.
 21. 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

MDCPS NETWORK SECURITY STANDARDS

- 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.
22. 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.
 23. 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."
 24. 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.
 25. 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.
 26. Personally owned computing devices such as desktops, laptops or Personal Digital Assistants (PDA) or portable / removable storage devices / media such as USB jump drives should not be connected to any MDCPS network without network administrator / site supervisor approval. These devices may carry applications, configurations, viruses, etc. that could pose a risk to the network or may be used to remove data from the network. School system techs may grant approval after, as time permits, certifying the device is not a threat to district networks. Techs are not required to bring the personal device into compliance unless directed to do so by their supervisor. For more information, see Section 4.2, Portable Devices below.
 27. Devices like routers, hubs, switches, firewalls, wireless access points, etc., whether personally or district owned, should not installed without prior approval from the site supervisor and ITS. Once approved, techs are required to bring these devices into compliance with these standards.
 28. 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 11. in this section).
 29. 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,

MDCPS NETWORK SECURITY STANDARDS

confidential data, user-ids, passwords, and information that can be used to access MDCPS network and/or mainframe systems left on these machines may fall into the wrong hands if steps are not taken to eliminate it.

30. The Office of Management and Compliance Audits, in concert with ITS, reserves the right to audit MDCPS locations for compliance with these security standards.

4.1 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 was 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 MDCPS wireless installations should be updated with any vendor patches supplying improved security features. If the device has no security available, it should be removed from the network and 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. 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).
3. When utilizing any outside wireless network or wireless service, Virtual Private Network (VPN) technology should be used.
4. 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.
5. ITS reserves the right to randomly scan or monitor for the presence of insecure wireless devices connected to MDCPS networks. ITS also reserves the right to disconnect any wireless device that appears to pose a threat to an MDCPS network.
6. At the very least, 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, and all default passwords should be changed. For details see the MDCPS Wireless Security Tech Note at:

http://techsupport.dadeschools.net/data_security/wireless_security.pdf

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

MDCPS NETWORK SECURITY STANDARDS

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:

1. 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.
2. Use of power-up and activity timer passwords is required on PDA's and notebooks.
3. 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.
4. Confidential MDCPS data should be set to "private" and "hidden" on Palm 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.
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, but 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 login 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. 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:

1. All authorized staff is responsible for protection of MDCPS assets, including computers and data.
2. MDCPS computer equipment is for MDCPS business and educational functions only. It is not to be used for unauthorized activities.
3. 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

MDCPS NETWORK SECURITY STANDARDS

- 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 physical or virtual access to administrative computers anywhere at their location. This also applies to descriptions and/or diagrams of MDCPS 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.
4. 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 ITS. Staff should also be careful not to expose sensitive data using the file-sharing capabilities of their computer.
 5. 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 MDCPS 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.
 6. 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.
 7. Security software (anti-virus programs, spyware and hacking software 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.
 8. Vendors or other outside agencies seeking access to MDCPS equipment or data are to be informed of these standards and ITS network administrators should be notified.
 9. 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.
 10. Site supervisors are responsible for ensuring that all policies are observed.
 11. 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 quarterly report showing the authorizations held by site staff are appropriate..

MDCPS NETWORK SECURITY STANDARDS

12. Authorized staff should be informed of MDCPS computer security standards. New or recently authorized staff should be informed during orientation. Use of MDCPS equipment and/or networks constitutes acceptance of these policies.
13. Any authorized staff approached with a proposition to violate these standards should notify their supervisor and/or ITS. This also applies to any authorized staff observing any activity that may be a violation of these standards.
14. 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.
15. 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.
16. District-wide security initiatives such as loading MacAfee E-Policy Orchestrator (EPO) anti-virus software on all network connected district computers must be complied with. Future district-wide initiatives may include patch-management software and/or desktop-management software.
17. 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 ad-ware 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 load 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 ad-ware 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 spyware / ad-ware and cleans it from the machine.
18. 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.

Acceptance of employment or contracts with MDCPS will signify acceptance of these standards by the user. Failure to comply with this or any MDCPS 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 MDCPS networked computers without a user-id and password.

MDCPS NETWORK SECURITY STANDARDS

2. MDCPS 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.
4. User-ids will be revoked when an incorrect password has been entered 3 times in a row within a 30-minute 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 MDCPS user ids if the employee is accessing data illegally or has been terminated.
9. Passwords will be 6 – 8 characters long, including at least 1 numeric character.
10. 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, 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", 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.
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 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.

MDCPS NETWORK SECURITY STANDARDS

20. 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:

1. Auditing/logging of such security-relevant information as logon and resource access violations
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

6.0 Changes To Standards

The ITS Data Security Department, in conjunction with other ITS departments (Network & Internet Services, Technical Support, Systems and Programming, etc.) 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 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 ITS 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.

MDCPS NETWORK SECURITY STANDARDS

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

MDCPS NETWORK SECURITY STANDARDS

Index

- 3DES. *See* encryption
- Access Point. *See* AP
- Active Directory Services. *See* ADS
- Administrative computers, 3, 6
- ADS, 3
- ad-ware, 11
- anti-virus, 6, 9, 10
- AOL, 6, 10
- AP, 8
- audio. *See* MPEG
- authorized staff, 1, 2, 9, 10, 11
- backup, 5, 9
- bandwidth, 4
- chat, 4
- Classroom computers, 6
- content filtering. *See* filtering technology
- copyright, 4
- Cracked software, 6
- desktop-management, 11
- dial-in, 5
- Digital Subscriber Line. *See* DSL
- disaster contingency plan, 5
- domain administrators, 3
- DSL, 5
- e-mail, 4, 6, 7, 10, 13
- encryption, 1, 7, 8, 13
- End User License Agreement. *See* EULA
- Enterprise Administrator, 3
- EPO, 11
- E-Policy Orchestrator. *See* EPO
- EULA, 11
- File Transfer Protocol. *See* FTP
- filtering technology, 6
- firewall, 3, 8
- FTP, 7, 12, 14
- Games, 4
- grade book, 6
- Group membership, 7
- Guest, 12
- Hacking software, 5
- Hotbar, 11
- Hotmail, 10
- instant messenger, 4
- Internet, 1, 3, 4, 6, 7, 9, 13, 14
- Internet Service Provider. *See* ISP
- Intranet, 9
- ISP, 6
- jump drives. *See* USB
- KAZAA, 11
- LAN, 3, 5, 13, 14
- licensed, 2, 8, 10
- local area network. *See* LAN
- mainframe, 2, 3, 4, 6, 7, 8, 13, 14
- modem, 5
- MP3. *See* MPEG
- MP4. *See* MPEG
- MPEG, 4
- Novell, 3
- owner, 13
- P2P, 11
- Palm, 9
- passwords, 5, 6, 8, 9, 10, 11, 12, 13
- patches. *See* update
- patch-management, 11
- PDA, 7, 8, 9
- Peer-To-Peer. *See* P2P
- Personal Digital Assistants. *See* PDA
- Personally owned, 7, 10
- PGP, 7
- physical, 2, 3, 6, 9, 10
- Pretty Good Privacy. *See* PGP
- RACF, 1, 2, 4, 11, 12, 14
- RAS, 5
- remote access services. *See* RAS
- scan, 5, 8, 9
- scanning, 1, 5
- screen saver, 6
- Secure Socket Layer. *See* SSL
- service packs. *See* update
- Site supervisors, 3, 10
- sniffer, 5
- spyware, 1, 10, 11
- SSL, 1, 5, 7
- Stolen, 1, 11
- Streaming. *See* MPEG
- TCP/IP, 3, 14
- Unlicensed, 10
- update, 11
- USB, 7
- video. *See* MPEG.
- virtual, 2, 6, 10
- Virtual Private Network. *See* VPN
- VPN, 1, 5, 8
- WAN, 3, 5, 13, 14
- web servers, 6
- wide-area network. *See* WAN
- Windows 2000, 3
- Windows NT, 3
- wireless, 1, 2, 8, 9