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 data classification guidelines 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 standard. 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 relies on computers and data processing facilities to store and use vast amounts of data. That data includes, but is not limited to, student records, personnel records, business, and accounting records. The proliferation of networks and Internet related informational activities means that this sensitive data is more conveniently available to authorized staff in ways unimagined in the past. The rapid increase in the use of this data may also place the security of the data at risk. The purpose of these guidelines is to ensure 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 Information Technology Services (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 the unauthorized access to 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

Unauthorized access and/or destruction of District data is a crime under the Florida Computer Crimes Act (Florida Statute §815.01).

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

- Lawsuits for negligent protection of 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 capacity or unfair advantage to third parties by unauthorized disclosure of lists and other business assets to vendors
- Liability for maintaining incorrect data (including State and Federal penalties)
- Errors in business decisions due to reliance on inaccurate data
- Negative publicity surrounding the use of incorrect data and subsequent regulatory enforcement
- Inability to process business transactions in a timely fashion

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 Policies, and decisions by senior staff and/or the data owners (see section 2.1 of this document). Pursuant to Florida Statute §501.171 and Board Policy 8351, the District will take reasonable measures to protect and secure data containing sensitive information in electronic form and shall provide notice of a security breach as required. "Data in electronic form" means any data stored electronically or digitally on any District or third party agent computer system or other database and includes mass storage devices. M-DCPS will also seek prosecution of individuals who commit computer related crimes as set forth in Florida Statute §815.06.

1.3 Background of M-DCPS Data Security

Historically, almost all M-DCPS data was kept on the M-DCPS mainframe at ITS and access was strictly controlled through the use of the mainframe IBM OS/390 Security Server (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, volunteers, and others

authorized by M-DCPS to use the specific M-DCPS computer systems, applications, and information required for the performance of their job duties and responsibilities, 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, switches, routers, hubs, wireless devices, 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
- Any equipment not owned by M-DCPS but connected to the M-DCPS network.

All M-DCPS staff and authorized non-staff must be aware of the risks and act in the best interest of M-DCPS. Failure to follow these guidelines may lead to the denial of access to M-DCPS data. 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 under the law. Failure to adhere to these guidelines may result in a violation of provisions set forth in Chapter 815 of the Florida Statutes.

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. For purposes of determining data sensitivity, PII (Personally Identifiable Information)/PI (Personal Information) shall be deemed sensitive and, therefore, handled in the appropriate manner. Moreover, personal information, as defined herein, is confidential, and not subject to public disclosure. Board Policy 8351 defines "Personal Information" as follows:

1. an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

    a. a social security number;

b. driver's license or identification card number, passport number, military identification number or other similar number issued on a government document used to verify identity;

c. a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to access an individuals' financial account;

d. information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

e. an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

2. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

The term does not include information about an individual that has been made publicly available by a Federal, State, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

PII/PI shall be collected and utilized by authorized staff for explicit business purposes only and/or as required or permitted by law. If collection or use of this information inconsistent with the intent of this policy is found to occur, appropriate disciplinary action will be pursued.

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, networking components (including wired and wireless infrastructure) and especially sensitive applications and data. Security includes, but is not limited to, lockable doors and windows, limited access, protection from water, fire, and the elements, alarms, access controls, and surveillance devices such as cameras and monitors. Site supervisors must take necessary and reasonable steps to protect all hardware and software assigned to their location.

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 Electronic 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 such as log-on information, resource access, and 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.

4.1 M-DCPS Network Systems Security

Network systems include any local area network (LAN), wide-area network (WAN), dial-up, Internet, servers, switches, routers, 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, 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 2008 (or above) operating system. Microsoft no longer supports Windows NT, Windows 2000, XP, or Windows 2003 and will not provide fixes or reports for vulnerabilities, including any new ones found. No Windows NT or 2000 servers are to be connected to the network and every effort must be made to remove Windows 2003 servers currently connected. Since these Operating Systems (OS) are unsupported, there is no anti-virus or patching available for them and they are, therefore, unprotected. Sensitive data should be moved to a server with a compliant OS. Applications should be updated to work on and be moved to a higher level OS. If an updated version is not available, vendors must be notified that they must provide an updated version of the application as soon as possible. Desktops and laptops connected to the network should similarly be migrated to Windows 7 or above to take advantage of higher levels of security.

2. The District employs Active Directory Services (ADS); Information Technology Services has established and maintains the root ADS for M-DCPS and determines local and group policy settings. All other District servers will be added to the ITS established Active Directory.

3. Active Directory Organizational Units (OUs) have been established for 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 Operating Systems no longer supported or patched are prohibited from being connected to any M-DCPS business network.

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

   M-DCPS Responsible Use Policy of the Network/Internet for staff
   http://www.neola.com/miamidade-fl/search/policies/po7540.04.htm

   M-DCPS Responsible Use Policy of the Network/Internet for students
   http://www.neola.com/miamidade-fl/search/policies/po7540.03.htm

   M-DCPS Board Policy regarding Copyright
   http://www.neola.com/miamidade-fl/search/policies/po2531.htm

   M-DCPS Board Policy regarding staff use of District e-mail systems
   http://www.neola.com/miamidade-fl/search/policies/po7540.05.htm

   M-DCPS Board Policy regarding student use of District e-mail systems
   http://www.neola.com/miamidade-fl/search/policies/po7540.06.htm

   The Office of Management and Compliance Audits (OMCA) web site,
   http://mca.dadeschools.net/IT_Audits.html

6. 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. Backup-up data should be checked for consistency.

7. 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.

Unauthorized individuals are not to have access, either physical or virtual, to production servers or any administrative computers.

8. 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:

    a. installing application passwords and timeouts,
    b. up-to-date anti-virus software,
    c. separate computers for teacher use only,
    d. 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,
    e. installation of anti-spyware applications when available,
    f. possible storage of grade and test data on removable (encrypted) media, and
    g. limiting unsupervised student access as much as possible.

9. 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. The timeout may be temporarily disabled by the local admin when the computer is to be used for presentations or other instructional activities but must be turned back on when the activity has been completed.

10. Classroom computers are defined as computers used by students. There are to be no administrative applications, especially mainframe sessions, installed on any of these computers.

11. Public facing content (web and otherwise) should be provided only through "hardened" Web servers using the latest OS and software updates. Web servers should have no other applications running on them and should be segregated from the rest of the M-DCPS network. Information on Web pages must be kept as current as possible.

12. 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.

13. 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.).

14. Wake On Lan should only be used for maintenance purposes and testing to abide by District initiative.

4.1.2 Data Access, Transfer and Communication

1. Network perimeter defenses are designed to protect the District. ITS will keep audit logs and review them actively for malicious activity. If access from outside of our network is needed an incident can be generated and approved by Data Security to grant VPN access.

2. Access to secure mainframe applications via the network requires RACF authorization.

3. When dealing with PII or sensitive data on a personal device and using a public network, Wi-Fi or Ethernet, a VPN and secure connections should be utilized to help prevent data from being compromised. Examples include user-ids, passwords, account numbers and financial information, student data deemed exempt from public release by state law, or Human Resource (HR) data.

4. Remote support should be turned on only when support is needed (and the user has given permission and or generated an incident, if applicable) and immediately turned off once the support has been provided. Most free remote tools are unsupported and have known security vulnerabilities. ITS recommends District technical staff use Dameware or RDP Protocol as approved remote support tools.

5. Confidential data taken from the District, whether via laptop or other mobile device, jump drive, removable media like a CD, 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) operations or e-mail transmission with the District in which confidential data is transferred are to be directed/required 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.

6. 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.

7. 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 network administrator and/or technician to ensure that this data is secure.

8. 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 Network and Internet Acceptable Use Policy, the Staff and Student E-Mail Policies, the Copyright Infringement Policy, the Network Security Standards or any other District policy, Board Policy or directive relating to user conduct. It should be noted that the District e-mail policies discuss the lack of privacy in the e-mail system at length.

9. Personal or vendor-owned devices such as desktops, laptops, mobile devices, 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/malware, 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. Any personal/vendor-owned device that will connect to the network will be considered unmanaged; these devices must connect to and adhere with the criteria of the Bring Your Own Device (BYOD) network. (See Section 4.4 BYOD – Bring Your Own Device below.)

10. Devices like routers, 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, ITS 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. ITS will disconnect, modify and/or confiscate any device not meeting these standards or when the device is being used inappropriately.

11. Sensitive/confidential data to be accessed via the Internet must be secured during transmission using encryption (See item 4, section 4.1.2 Data Access, Transfer and Communication).

12. Any computers or networking devices removed from service in the District must have the hard drives cleared or purged (as per the NIST Guidelines for Media Sanitization) of software and data before they can be sold, given away, or disposed of. This process must be documented via the District's standard incident reporting system. A variety of commercial as well as open source tools (such as DBAN) exist to help facilitate this process. In the case of switches/routers/etc., the configuration must be wiped. 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.

13. 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. Although District bids and contracts may specify that hard drives be removed or cleared/purged/degaussed by the vendor when the machine is being taken out of District use, local supervisors should confirm that this has been done.

14. 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 and/or business purpose and prior approval. 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 without an instructional or business purpose 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 5, 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. See also School Board Policy 2531, Copyrighted Works.

3. Streaming audio and video is basically the same type of data as MPEG, but is sent as 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 or business purpose and site supervisor approval.

4. Voice over IP (VoIP) applications are prohibited without a valid educational or business purpose and authorization. These applications may consume large amounts of bandwidth and require client software that can introduce security vulnerabilities unless they are updated on a regular basis.

5. "Hacking software" has been designed to allow unauthorized persons to infiltrate computers on the network, view and modify data, and spy on a user's keystrokes in an effort to get user-ids and passwords, among other things. 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 or does not meet District compliance.

   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.

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

7. 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, sites whose content would be in violation of School Board Policies (e.g., Anti-Discrimination/Harassment 1362, 5517), 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. Internet content filtering audit logs showing Internet activity and sites visited by users may be reviewed at any time. Employees who violate District policies regarding inappropriate use will be subject to discipline up to and including termination of employment.

8. 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. Supervisors must comply with District guidelines issued by School Operations, regarding system authorizations given to staff. The following is an example of applications that fall into this category:

    a. Mainframe academic grade and attendance update

    b. Grade Book Manager and Attendance functions

    c. Payroll data entry and approval

    d. Requisition data entry and approval

2. Providing access to IT systems within M-DCPS follows the principle of least privilege. Users are automatically provisioned with basic access to systems such as the employee portal, email, and the employee's work location collaboration site.

Access to other systems must be provided by the work location supervisor utilizing AAAA, Quad-A, or Quad-A+; in instances where a supervisor is unable to utilize any of these mechanisms to grant required access, a formal request should be submitted by the site administrator to ITS Data Security utilizing the District.

4.1.5 Periodic Review of Systems Access by Site Supervisors

1. The determination as to whether or not access is appropriate for a specific user is left to the discretion of each site supervisor. However, access granted must be in compliance with District guidelines, School Board Policy, and applicable laws. It is critical to note that providing read-only access to systems, without the explicit ability to change or manipulate data, may increase the District's risk of exposure, particularly as it applies to Personally Identifiable Information (PII) of both students and employees, and can lead to identity theft. Therefore, read-only access should be granted just as carefully as those authorizations which allow changes to system data.

   Authorizations must be reviewed monthly by site supervisors. Unnecessary authorizations/roles can be removed using the same mechanisms used to grant initial access (AAAA, Quad-A, or Quad-A+). In instances where these systems are inaccessible/unavailable or other impeding technical issues arise, a formal request should be submitted by a site supervisor via the District's standard incident reporting system (i.e. HEAT) to ITS Data Security for assistance.

2. Site supervisors are reminded that legacy RACF authorizations are listed in the "Authorizations for Employees by Location" report (Product Number T0802E0101). This report is generated monthly and available through the Control-D Web Viewer on the Intranet.

3. The SAP Security Roles Report provides a mechanism for site supervisors to review SAP roles. The report is available on-demand, and must be reviewed monthly in the same manner as the RACF report. The SAP roles report can be found within the ERP Administration tab, in the site supervisor's employee portal.

4. As stated above and for audit purposes, site supervisors are required to review and retain a signed and dated copy of both the RACF and SAP Security Roles reports on a monthly basis to document the review, showing any changes made, and that the authorizations held by staff are appropriate (See section 4.1.4 Authorizations and Access). Reviewed RACF and SAP Security Roles reports are to be initialed and retained for 12 months.

4.1.6 Access to Systems by Vendors, Consultants, Contractors, or other "non-employees"

1. For purposes of assignment and accountability to systems access, the site supervisor of the work location requesting access on behalf of consultants, contractors, or other "non-employees" becomes the "owner" and is responsible for periodically verifying that systems access remains necessary and appropriate.

2. Requests to provide, cancel, or make changes to the account of non-employees should be submitted to ITS Data Security by the site supervisor via HEAT.

3. All access provided to non-employees pursuant to these requests will be automatically disabled six months after the date of initial request (or the length of the engagement if less than six months as stated within the request). Upon account expiration, a subsequent request to re-enable/extend access must be submitted via HEAT.

4. Access granted via a re-enable or extension request also becomes subject to the six-month/length of engagement expiration policy. If an engagement ends prior to the specified duration of the original request, the work location's site supervisor must request the timely termination of access utilizing HEAT.

4.1.7 E-Mail

Users are reminded that the District Staff E-Mail Policy 7540.05 (See section 4.1.1 Network Structure, Hierarchy, and Requirements, number 5) 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 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. Employees are required to retain public records that are received or transmitted through the District e-mail system for the period of time specified in the applicable State retention schedules (Policy 7540.05).

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 approved security available, it must be replaced or removed immediately. New installations should use only products with high-level encryption. In all cases, the installation's security features must be turned on.

2. All wireless installations must be approved and managed by ITS. This includes all school and administrative sites. All unknown, unapproved, or interfering wireless nodes will be subject to limited or no access. This includes removal, confiscation, and/or blocking of non-compliant nodes. Wireless nodes include, but are not limited to, wireless access points, wireless routers, ad-hoc devices, wireless printers, wireless storage devices, and other such wireless peripherals.

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.

4. Site supervisors and technicians should check that other staff does not install rogue devices. 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. Every effort should be taken to avoid tapping into outside wireless networks.

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

7. 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.

8. ITS is authorized to randomly scan or monitor for the presence of unauthorized, incorrectly configured, 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, removed, and/or blocked.

9. M-DCPS business wireless devices should be purchased through the M-DCPS bid process. Devices purchased through the bid are enterprise capable, have greater capacity, and generally include surge protectors, installation, and support. Additionally, in some cases wireless devices are covered by e-Rate, so the cost to the school may be about the same as the low-end devices purchased outside the bid.

10. 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, except for an ITS approved and configured Service Set Identifier (SSID) connecting to a restricted BYOD wireless network,
    - Wi-Fi Protected Access 2-PreShared Key (WPA2-PSK) with Advanced Encryption Standard (AES) encryption should be turned on, configured, documented, managed and/or otherwise approved by ITS,
    - 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.

11. No device can participate in an ad-hoc network or reside behind or act as a firewall or Network Address Translation (NAT) device while connected to an MDCPS network.

4.3 Portable Devices

Use of laptop/notebook computers and other mobile devices 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 mobile devices 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 mobile devices and notebooks.

3. All portable devices, including smartphones, 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 3rd-party application and may be file-specific, folder-specific or whole-disk. Note that some versions of Windows, 3rd-party vendors and hard-drive manufacturers now provide these capabilities. 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. Data on damaged mobile devices should always be cleaned if at all possible before the device is sent to a repair facility or disposed of.

11. Bluetooth devices connected to mobile devices and cell phones should have built-in security turned on as nearby Bluetooth devices may pick up their signals.

4.3.1 Digital Convergence – District-owned Devices

As part of its Digital Convergence Initiative, Miami-Dade County Public Schools has deployed mobile devices (tablets and laptops) to select grade levels and subject areas, and to address technology needs in support of District programs and initiatives. Students who are issued District-owned a take-home mobile device are required to have a parent/guardian signed contract (the District's current year Mobile Device Agreement); the agreement can be found at http://digital.dadeschools.net/contracts.asp.

4.4 BYOD – Bring Your Own Device

A BYOD device is defined as a wireless end device (laptop, tablet, smartphone, blackberry, e-reader, etc.) not purchased or managed by M-DCPS, which is used by students, staff, parents, or others to connect to an M-DCPS approved public access wireless network. The BYOD network is defined as a wireless network physically and virtually separated from the MDCPS internal network. The device must be able to support security settings of WPA2-PSK with AES and authenticate against a web based captive portal. A captive portal is an initial web page used on the District's BYOD network that requires users to sign in, review, and accept the District's Responsible Use Policies before being granted access to the network. See School Board Policy 7540.03.

Each user must connect/authenticate with a unique District provided user account. No generic logins will be allowed. No unencrypted transmissions, peer-to-peer communications or ad-hoc networks will be allowed. Users must agree to the District's Responsible Use policy. The District reserves the right to collect identifying information such as MAC addresses, serial numbers, etc. if necessary. Student use of the BYOD network requires a signed "Personally Owned Computing/Network Device Acceptance of Responsibility and Device Use Agreement Permission Form" (FM-7523).

The District's BYOD network will be subject to best effort bandwidth and may be restricted and/or disabled if necessary. It will be configured to access internet resources only. BYOD applies only to the BYOD wireless network established and configured by ITS. No BYOD device will be permitted on the wired network.

Only sites meeting the following criteria will be eligible for BYOD network implementation:

- ITS approved, configured, and managed Intrusion Prevention Systems; (IPS) device for BYOD;
- ITS approved, configured, and managed router for BYOD;
- Enterprise level wireless controller infrastructure.

Wireless security on enterprise devices must include at least,

- captive portal,
- WPA2-PSK with AES,

- Virtual Local Area Network (VLAN),
- Access Control List (ACL), and
- Firewall support.

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 cannot 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.

5. Authorized staff must see to it that students or other unauthorized persons never have unsupervised physical or virtual access to administrative computers and applications anywhere at their location. This also applies to descriptions and/or diagrams of M-DCPS network infrastructure and security audit findings.

6. 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.

7. 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.

8. 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.

9. 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 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 attachments. This is due to the threat to M-DCPS network resources from malicious programs sent by hackers via attachments in e-mail.

10. 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 needs access to connect to their own company's systems. This would allow ITS to provide content filter bypass and/or additional services as necessary.

11. Site supervisors are responsible for informing authorized staff and users of these policies and security responsibilities. In addition, site supervisors are required to review and retain a signed copy of the RACF and SAP Security Roles reports monthly, showing that the authorizations held by site staff are appropriate, especially in regard to high risk (See sections 4.1.4, 4.1.5, and 4.1.6).

12. 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.

13. 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.

14. 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.

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. 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.

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. Malware can be easily introduced to a user's PC by downloading or installing illegitimate software, or visiting infected websites. Be sure that your browser preferences are set so that software cannot be loaded on your computer without notifying you.

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.

19. The M-DCPS Responsible Use Policies delineate the proper use of the Internet by students and staff and define 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 or inappropriate material 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.

20. Users of M-DCPS computers are responsible for backing up their own data stored locally on the desktop, My Documents, etc. Users should put documents that need to be shared or that are mission-critical on the appropriately secured network share. Site-based technicians shall be responsible for backing up information stored on network shares located on locally managed servers.

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. Employees must annually acknowledge that they have read and understand these guidelines.

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, Portal session (or any application requiring user authentication), or will be leaving a computer unattended, they must log off of the computer, Portal session, or application, or lock the computer (CTRL-ALT-DELETE, Lock Computer) to prevent their account from being compromised. This is particularly important for teachers – leaving their account open on the computer may provide students and other unauthorized users with access to their grade book, e-mail account, personal information on the District Portal, and other sensitive/confidential applications and data (see 4.1.1.9).

4. When creating the questions and answers for their profile in the District's user password reset self-help application, users should be careful not to choose questions for which the answer is commonly known or easily guessed. For example, if a teacher has discussed in class that they were born in "New York", or that their favorite sports team is the "Dolphins", they should not use these questions in their profile. Less commonly known questions may include the user's father's middle name or the user's first car. Staff should also be aware that students may try to draw out answers in casual conversation.

5. User-ids will be revoked when an incorrect password has been entered a certain number of times within a specific timeframe.

6. User-ids will be revoked on all computer platforms when a user is terminated or transferred.

7. User-ids may be revoked, cancelled, or suspended at any time.

8. 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.

9. 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/when the password should be changed. Notification of an impending password change deadline will be provided whenever possible.

10. Users are restricted from reusing their last 6 passwords.

11. 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.

12. Users may change their password at any time.

13. 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.

14. Staff must not engage in any activity that may reveal or otherwise compromise their own or another user's password.

15. 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.

16. 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." The user-id and password of locally managed servers and applications 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.

17. Under no circumstances should any individual, including supervisors, ask for any other individual's network password or CICS password.

18. Avoid transmitting or storing passwords in clear text whenever possible. If available, password encryption should be turned on.

19. Local Windows passwords are not secure and thus only the network log-on should be used for security and authentication.

20. In the interest of personal security, users should be aware 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 via HEAT. 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.