NETWORK SERVICES

In the past, an M-DCPS school or administrative client site was limited to mainframe computer applications. Now, personal computers are everywhere. Through computer networking technology, users at a client site can access many different types of services (such as the Internet and mainframe applications) using a common network infrastructure. This technology, the Wide Area Network (WAN), has quickly become a necessary component of the information access requirements for all M-DCPS-client sites. The M-DCPS WAN includes approximately 450 school and administrative sites. WAN connectivity provides the pathway for access to critical business systems as well as student, educational research. Future utilization of the WAN will include access to data warehouse information databases, integrating voice (phone) system technology, as well as an increased access to more sophisticated Internet-driven applications.

Services Provided

Network Services staff members provide a large number of technically oriented services that relate to computer networking technology. Some of the major services provided include:

- Daily management and operation of the M-DCPS WAN
- Management and operation of the ITS “core network”
- Management and operation of the downtown, SBAB administrative network
- Technical support to school/administrative network administrators
- Technical support for all ITS-/SBAB administrative servers
- Network security including firewall management, intrusion detection, prevention, and remote-site security scans
- Technical support for other ITS departments such as Application Solutions, and
- Technical Support, field service technicians, and Internet Services.

Network Technology Standards

The following information will discuss the technology standards used by Network Services staff members. In addition, Network Services staff members recommend these standards as guidelines to other M-DCPS administrative and school sites that seek to implement network technology of this type. For the purposes of this document, two main areas of technology will be discussed: physical network infrastructure and logical network design.

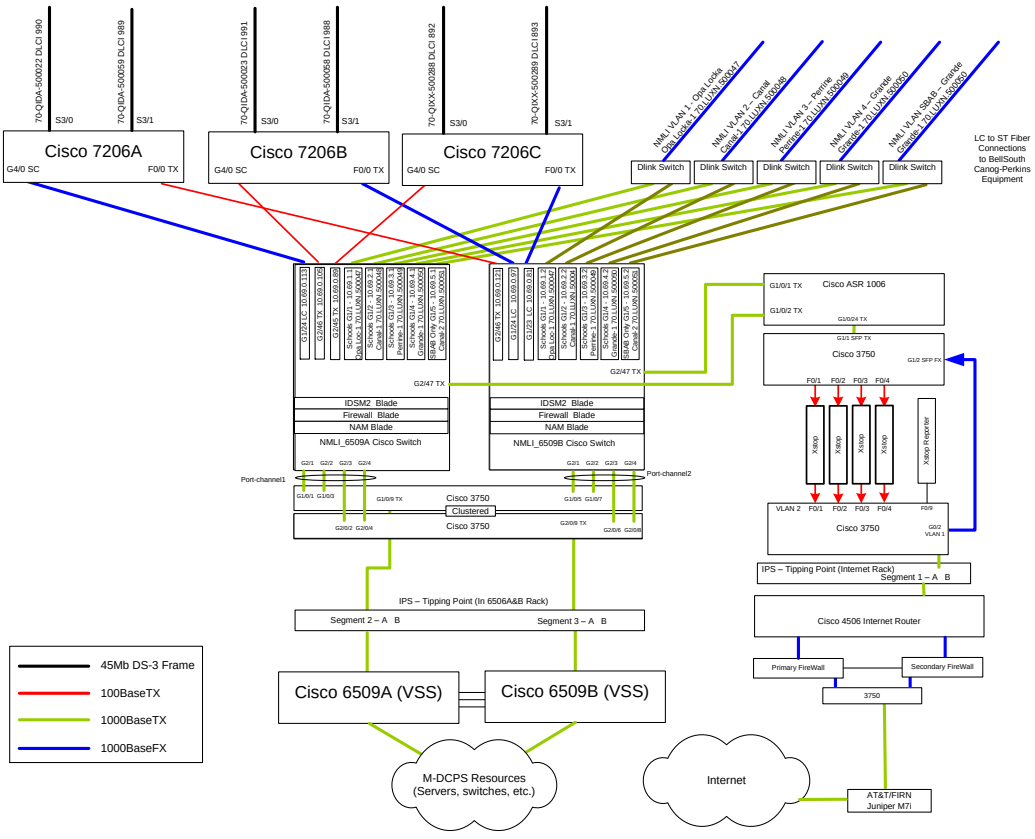
Physical Network Infrastructure Standards

Network infrastructure has to do with the "physical structure" of a network. That is, the various components such as architectural design, physical wiring, wiring concentrator devices and data communications circuits that form the infrastructure upon which data travels. The following standards are used:

Design Overview

The design of the M-DCPS WAN is a "hub and spoke" model. The ITS core network is the "hub." Each remote school/administrative site network connected becomes a "spoke" in this design. As the hub, the ITS core network provides remote sites with access to services such as content-filtered Internet and access to fiscal and student applications on the ITS mainframe computer. Appropriate network security technology has been deployed to protect the ITS core network from unauthorized access. This includes firewall technology facing the public Internet, as well as intrusion detection devices that protect possible inside hacking from M-DCPS, remote-site networks.

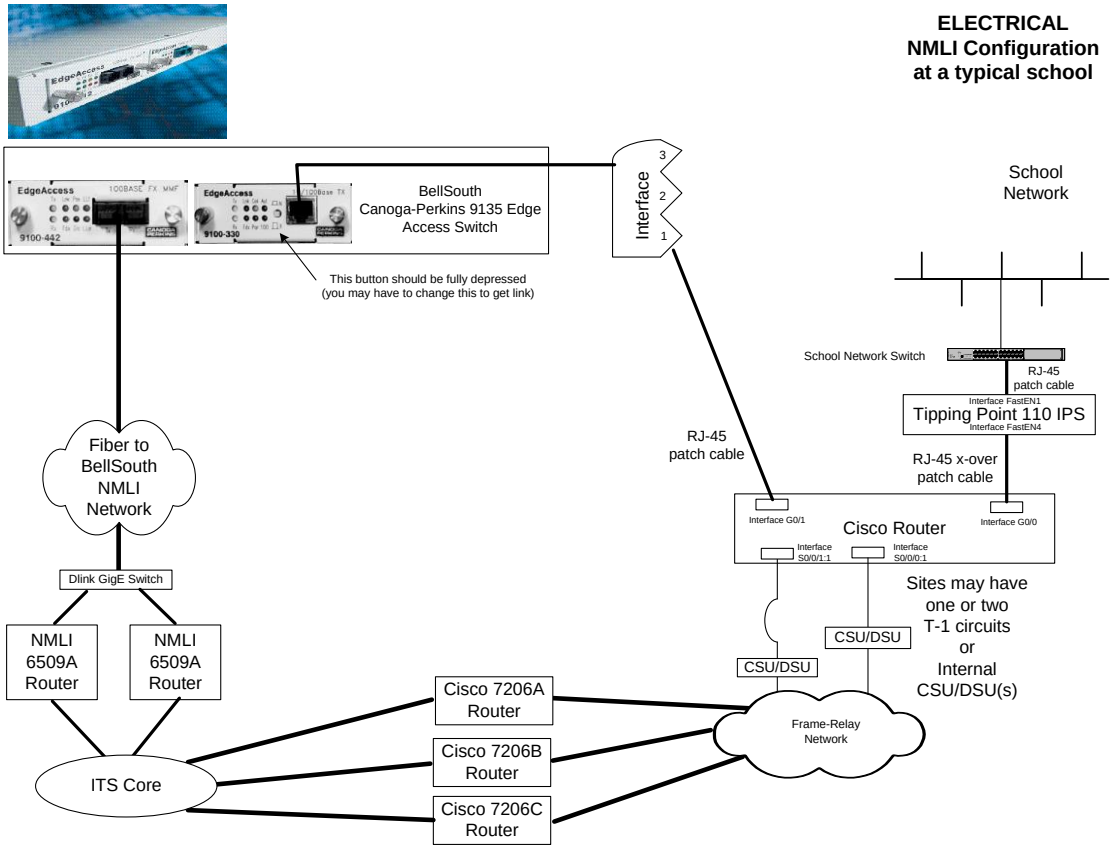
Please see Network diagram below.



Data Communications Technology

Remote sites connected to the M-DCPS WAN currently use a 10 Mbs NMLI (Native Mode LAN Interconnection) at remote sites with a T1 frame-relay data communications circuit as backup. Several high bandwidth locations have 100 Mbs (for example, Robert Morgan Ed. Center, Food Services, and Facilities Operations at Toys-R-Us). The primary connection between ITS and the SBAB network is 1 GB NMLI. The local telecommunications service provider supplies this circuit. ITS provides the appropriate CSU/DSU (data modem) and router device to enable the remote site to communicate with the ITS core network. To maximize data packet travel, Network Services staff members utilize Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP). Network Services staff members configure the router to include a security login and password to prevent unauthorized access to this device. One goal of Network Services staff members is to reduce the number of "routable" protocols that must be supported. For this reason, Network Services staff members promote the Transfer Control Protocol/Internet Protocol (TCP/IP) as the standard network protocol for LAN (Local Area Network) and WAN functionality.

Refer to the diagram listed below.



Wiring

All normal “hard wire” installed for data/voice communication connections should be at least solid copper CAT 5. In addition, fiber optic cable should be used when appropriate to overcome distance limitations and/or bandwidth requirements. Wireless technology can be incorporated to facilitate remote buildings when/where installing hard wire is not feasible such as portable or detached buildings. All wireless technology deployed must be configured according to the security standards set in the Network Security Policy available at: http://techsupport.dadeschools.net/data_security/datasecurity.asp.

LAN Protocol

Network Services staff members endorse the use of the Ethernet LAN protocol. This is the industry’s standard protocol. The LAN supports 10 Mbs, 100 Mbs, and gigabit versions (1 GB and 10 GBs).

Concentrator Devices

Switched 10/100/1000 devices are the normal standard recommendation for end-user connection. LAN backbone requirements may also require gigabit switch capacity. Switch technology provides for the facility to segment the site network thus allowing for more efficient operation and better manageability.

ITS Core Network Security

Officially, the responsibility of Network Services staff is to administer and support the ITS core network, as well as administrative LANs within the ITS work location and the downtown SBAB building complex. Traditionally, for a remote site, the responsibility of Network Services staff members (in terms of management) ends at the point where the ITS-supported router device attaches to the site’s LAN.

Consequently, Network Services staff treats M-DCPS remote sites as non-secure connections. For this reason, Network Services staff installed a series of intrusion prevention devices, including firewall technology facing the connection to the public Internet, to detect and deal with “hacker”-type activities which may originate at an M-DCPS, remotely connected site. The security guidelines for the firewall deny all access and permit only exception traffic.

ITS Core Network Security (continued)

In addition to the previously mentioned security technology, Network Services staff performs random security scans of remote sites to identify potential network security issues. These security scans are designed to reveal: 1. unauthorized activities (as defined in the Network/Data Security Policy accessible at: http://techsupport.dadeschools.net/data_security/datasecurity.asp); 2. activities that may be occurring on a remote-site network; 3. servers not configured correctly; or 4. other, installed network devices. Upon detection of inappropriate activity, Network Services staff will follow up with either the school-site administrator and/or staff from the Office of Professional Standards.

ITS Core Network Physical Security

All servers, switches and other core network technology components are in a secure "server room," accessed only by authorized personnel. Within the server room, locked cabinets contain the critical-core network devices. Each member of Network Services and the Computer Operations Manager receives keys to the cabinets. Access to the ITS computer room is through a security-card scan only. Remote-wiring closets should be locked at all times. All devices (desktop and servers) that are used to host applications that are run as regularly scheduled production jobs should be physically located in the computer room complex.

IP Address Conventions

Each TCP/IP environment requires the use of a unique IP address for each device to be addressed on the network. M-DCPS is the owner of the "class B" address scheme. To accommodate the many thousands of devices throughout the M-DCPS WAN, Network Services staff members adopted the use of dynamic, address-assignment technologies such as Dynamic Host Control Program (DHCP) and Network Address Translation (NAT). Specific devices will be assigned a permanent, fixed-IP address depending upon need. These devices are traditionally switches, routers, and servers.

Internet Content Filtering

AT&T provides access to the Internet to M-DCPS employees and students. At http://techsupport.dadeschools.net/data_security/datasecurity.asp everyone can access the District's Acceptable Use Policy which dictates the appropriate use of the Internet. To facilitate the implementation of this policy, Network Services staff members provide content filtering technology that blocks individuals from attempting to access predefined, inappropriate sites. The Internet Services group administers the content-filtering technology to adhere to the CIPA (Children's Internet Protection Act) guidelines.

Remote Access

To provide M-DCPS employees with remote access to the Internet and other administrative-type functions, Network Services staff provides access through a VPN (Virtual Private Network) URL (Uniform Resource Locator, a web address). Users must apply for this service through the Internet Services department of ITS by clicking on http://www.dadeschools.net/request/. Network Services staff members issue approved users a login-authentication ID, password, and an IP address. ITS staff manages these users through Cisco's TACACS (Terminal Access Controller Access-Control System) software platform.

Network Management Technology

WhatsUp Gold and Orion Solar Winds are the main technology platforms used to manage devices on the ITS core network. In addition, staff uses HP to monitor and maintain ITS ADMIN server hardware. As a supplement, the native-device management and configuration interfaces are used to manage and configure various devices on the network, such as switches and routers. Network Services staff members work with personnel from other ITS support departments to share the responsibility of "round-the-clock" network monitoring; this includes all production servers, routers, and switches.

Logical Network Design Standards

Design Overview

Logical network design has to do with the manner by which network resources (users, servers, printers and data shares) are organized and managed. An important part of this design is the capabilities which are built into the network operating system (NOS) software. Network Services staff members have standardized on Microsoft's Windows Server platform as the NOS of choice. All ITS and downtown network users are organized into one domain called dadeschools.net. Within the dadeschools.net domain, various user groups have been created which reflect the different administrative work locations connected to the network. Within a specific user group, one or more data shares may be created and printers defined so that users may share these network resources. Optionally, a user group may wish to operate its own member server to facilitate a specific need or application within the work location. In all scenarios, ITS staff will maintain administrative control of the end-user accounts; although, there are some exceptions to this rule.

ITS has created another domain, participate.local, to allow students, parents, and community members to access the Portal and all its resources. This domain adheres to the the same high standards of privacy and security that characterize District applications.

Logical Network Design Standards (continued)

Design Overview (continued)

Strategy for Domain-Trust Relationships

Network Services' policy states that trust relationships with other domains are normally undesirable. However, Network Services staff members remain responsible and accountable for the activities of other domains that have developed within ITS' administrative network environment. To work with these departments outside of ITS and their established domains, Network Services staff members maintain minimal trust relationships, normally limited to the dadeschools.net as the trusted domain. This minimizes the risk associated with domain-trusting activities.

Server Specification

Server hardware must be purchased from a "bid-approved" vendor. Typically the server should be minimally configured to support data redundancy (RAID 5) and provide for an attached, data-backup device (for example, tape drive). In addition, a form of vendor-recommended, hardware-management software should be utilized. Network Services staff has standardized on HP hardware for server functionality and uses their Insight Manager software to manage server hardware. Network Services staff provides generic "minimal server specifications" for other M-DCPS sites.

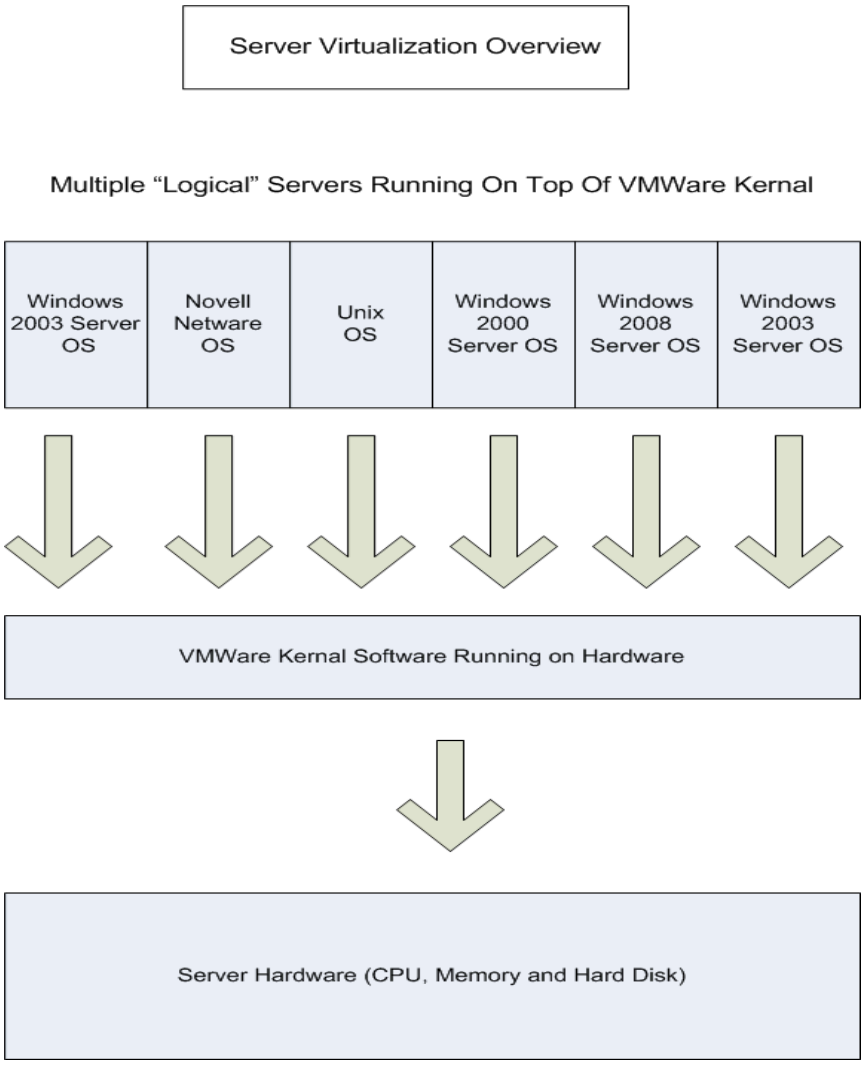
ITS has standardized on a virtual server environment, hosted on an enterprise-class blade server connected to a SAN (Storage Area Network). Exceptions will be evaluated and handled accordingly.

Network Services was an early adopter of server virtualization technology. This technology is based upon a base virtualization software application such as VMware being installed on the server hardware.

This virtualization software can then "host" multiple occurrences of various "logical" servers using traditional server-based operating system software such as Windows 2003, etc. In effect, multiple "logical" servers can be hosted on one "physical" server and the physical server's resources such as CPU, memory, and hard disk are "shared" by the multiple "logical" servers being hosted. The ROI (Return on Investment) is readily apparent in a more efficient utilization of hardware resources. In addition, indirect savings occur due to a reduction in electrical power consumption and cooling on a server-by-server basis.

Server Specification (continued)

At the time of this writing, Network Services is hosting over 800 virtual servers on over 60 physical servers. The range of applications includes the HEAT trouble ticket system, District Exchange email system, and Gradebook application in both production and development environments. See the diagram below for an overview of server virtualization.



Power Fault Tolerance

ITS has installed an Energy Center that provides power and redundancy for the network and server infrastructure. Services are provided 24/7, as the center was designed to withstand any countywide emergency.

Data Backup and Restoration

ITS uses an industry standard application for the daily, weekly, and monthly backups. End-user data on ITS-controlled servers is backed up based upon the requested schedule of the applications' manager. This schedule of the backup application is automated, and also backs up many servers simultaneously. The application will retry a failed backup six times before failing the backup job for that particular server. The application manager is notified via email on successful and failed backups.

The majority of ITS servers are virtual and a server image backup is performed, which gives ITS the ability to restore this complete image of the server when needed.

Starting every Friday and depending whether it is the end of the month, the backup application will start the weekly or monthly backup of servers and data. This process takes all weekend long to complete. Once the last backup has completed, the tapes used during this process for the weekend are ejected from the tape library and then are shipped to an off-site facility storage for a minimum of one week. Tapes can be recalled back to ITS if needed for a restore, that can be done by submitting an email to Computer Operations staff, who will recall the requested tapes.

Staff members perform a special, full backup of all data when there is a hurricane or other disaster warning. Currently, the Network Services backup team uses Symantec Netbackup software to provide backup functionality and uses Iron Mountain for their off-site storage facility for tapes.

If needed, ITS restores production data to servers from backups. This ensures the validity of the backup process as data is restored and utilized without incident.

Server Anti-virus Protection

All ITS-managed servers that contain end-user data have anti-virus software installed. Before any document is saved on the server, the anti-virus software scans the file contents for viruses. In addition, the software also scans on a weekly basis the contents of all user folders and shares to protect against virus infection from end-user desktops. The appropriate Network Services staff receives the virus scan results for analysis and then notifies end users if any infected files have been detected. Staff members also advise the end users to have their desktop computers checked for possible virus infection.

Patch Management and Anti-virus Updates

In order to ensure the entire network environment is up-to-date with patch management and anti-virus software, staff members from Network Services, Data Security, and Change Management met to develop new ITS standards. As a result of this meeting, all new servers, both those managed by District/ITS staff or vendors, are required to be built/configured with patch management and anti-virus installations. Change Management has partnered with the other ITS teams to create an effective strategy to retrofit existing servers that do not have patch management or anti-virus software installed.

In order to ensure that server environments are updated and patched in a timely manner, the patch management client will be installed whenever a new server is configured. Application owners can manage when patches/updates are applied to their servers through the console.

Application owners can request the client software through a HEAT Self Service ticket from http://heat9-web.dadeschools.net:8180/HeatWebUI/hss/HSS.html. It is the application owner's responsibility to contact the vendor for third-party applications to determine when patches/updates can be applied. Audits will occasionally be performed and if any vulnerabilities are discovered resulting from non-adherence to this policy, ITS reserves the right to immediately shut down the application and its host environment.

Additionally, District-approved anti-virus software will also be installed as part of a new server request. Exceptions to this guideline, from application owners, including vendors, must be requested in writing. The written request must be forwarded to Change Management and a staff member from Change Management along with the Chief Information Officer will review the request. Application owners will need to work with the Network Services team to configure when virus scans are scheduled.

Email Application

To facilitate electronic communication, Network Services staff members use Microsoft's Exchange email application which supports all major email message protocols. The Exchange email application also includes a calendar with its corresponding features and contacts with its management functions. Staff members at Network Services also scan all inbound- and outbound-messages on the servers with anti-virus and spam-detecting software.

End-User Devices

ITS staff members control all network connectivity to the administrative network. Through http://heat9-web.dadeschools.net:8180/HeatWebUI/hss/HSS.html, the link to the District's HEAT ticket system, end users request that desktop PCs, printers, or other devices be connected to the network infrastructure. ITS field technicians then carry out the service. Network Services staff members work with ITS field technicians to resolve any technical problems during this connectivity process. It is the end user's responsibility to ensure that the connected desktop has the appropriate anti-virus protection and that critical data kept on local, hard drives are being backed up accordingly.

Procedures Related to Network Services Operation

Many of the daily tasks of the Network Services staff members have to do with the operation and/or management of network technology. These procedures require minimal interaction with users in other departments and are clearly documented within the software documents related to the specific technology. For example, the procedure used to configure a Cisco 2621 router is clearly defined in the technical manual for this router.

Firewall Exclusion Requests

Usually, attempts from outside individuals/organizations to access M-DCPS resources are blocked. Staff members deal with exceptions, as needed.

Procedures for Processing Suspected Network Abuses

Network Services staff members need to follow the following procedures for processing suspected network abuses (for example, network scanning, access to inappropriate sites, etc.):

1. Upon detection or report of an incident, advise Network Services of the incident. Based upon the nature of the incident, staff members from Network Services and Data Security will work to address the incident and take the appropriate action(s). Network Services staff members will also advise ITS upper management of the incident, as soon as there is a clear understanding of the situation.

2. Based upon the nature of the incident (administrative or criminal), a management decision will be made as to the disposition of the incident. At that time, the corresponding incident documents may need to be made available to staff members in M-DCPS, Department of Professional Standards, or School Police.

ITS Core Network and Remote Sites Network Scans

There are over 400 remote sites connected to the M-DCPS WAN. As previously mentioned, Network Services staff members view all sites that are not under its control (all except ITS and downtown SBAB) as un-trusted and non-secure. To help identify possible, network-security risks, remote-site servers that are not configured correctly or other types of network issues, Network Services staff members perform periodic scans of all remote-network sites, as frequently as possible. In addition, Network Services staff will, at the request of the administrator of a remote site, visit the remote site and perform a more intensive analysis of the site's network and make recommendations as to how to correct noted deficiencies.

Technical Support for Remote Clients Sites

Each school's LAN is controlled by ISS (Infrastructure and Systems Support) which in turn is supported by Network Services. In line with this philosophy, Network Services staff members offer technical support in the areas of server installation, configuration and management, as well as network troubleshooting, including on-site visits.

Future Vision

Network Services staff members strive to empower M-DCPS-network administrators to manage their daily network functions. Remote sites need to host critical applications and data to minimize security risks and increase efficiency. To better coordinate and maintain services, M-DCPS' administrators need to create and support a central network management environment that will maximize efficiency and minimize risks. In preparation for this, Network Services staff members investigate and pilot new technologies designed to accomplish these goals.

DATA SECURITY

The Data Security Department safeguards the District's information assets including the mainframe, the network and the Internet. M-DCPS employees can access additional information about the department by clicking on http://its.dadeschools.net/dataSecurity/data.asp. The goals of the Data Security Department are to provide:

1. Protection of data from unauthorized destruction, modification, disclosure or use, whether accidental or intentional.

2. Smooth implementation of data security procedures through a phased plan, which includes progress reviews and approvals by the Data Security Review Committee.

3. Cost effective controls through analysis of risks and audit reviews.

Responsibility

Because of the enormous diversity and amount of information stored at ITS, from confidential student information to public records of financial information, and from mainframe to network, available at over 1000 sites throughout the District,

M-DCPS utilizes a decentralized security model in which a site supervisor is required to determine appropriate authorizations and/or roles for their respective staff at his/her discretion. As such, site supervisors are required to periodically review current authorizations for validity. The role of ITS is to provide the mechanism for supervisors to review and manage those roles. As stipulated by policy 5.0.13 (Staff Security Responsibilities) of the Network Security Standards, ITS currently produces an automated monthly report made available to all site supervisors electronically. This report currently details RACF and Active Directory application roles and site supervisors are required to review the reports per policy. Each site is ultimately responsible for the accuracy of the authorizations given.

Chief Information Security Officer

The Chief Information Security Officer shall:

- Ensure the integrity of the Resource Access Control Facility (RACF) as installed and utilized at M-DCPS.

- Ensure the integrity of the Active Directory System (ADS) and Group Policy or any other facility used to manage network assets and account security.

Chief Information Security Officer (continued)

The Chief Information Security Officer shall (continued):

- Assist the authorizing administrators in evaluating their data requirements, security risks, and security responsibilities.
- Implement and administer procedures to control data access and minimized security risks.
- Continually monitor the security system for:
    - Violations, unintentional repeat offenders and deliberate attempts to circumvent
    - Availability, the security system (RACF, ADS, and Group Policy) must be available whenever the network is available.
    - Currency, the security system must accommodate new applications and new technology.

Authorizing Administrators

Each site connected to the ITS network has a designated authorizing administrator. He or she has been given the authority and responsibility to directly administer certain data security system functions. These functions are:

- To determine which of the applications available at ITS is needed for the operation of their location.
- To designate (authorize) which of their employees shall be able to access each of those applications.
- To change the access authorization of their employees as necessary.

Due to the sensitive nature of many of the authorizations given to ITS staff, authorizing administrators must review their staff's access quarterly, mark any changes on the report (T0802E0101) either electronically or as a hard copy.

Users

Once employees have been authorized to access any of the applications at ITS they assume the responsibility to:

Users (continued)

- Use that authority in the proper function of their employment by M-DCPS.

- Maintain their password and not allow others to use their account.

- Follow the requirements set forth in the Network Security Standards, the Network Acceptable Use Policy, the staff E-Mail Policy, the Copyright Infringement Policy, and any other District directives regarding computer use. Up-to-date links to these documents are available at the following Web site:

  http://techsupport.dadeschools.net/data_security/datasecurity.asp

- Pursuant to the Network Security Standards, individuals storing confidential/sensitive information on laptops or other portable media must take the appropriate precautions to ensure that such information remains confidential. ITS recommends the use of EFS to encrypt files of this nature. Additional information regarding EFS (including a brief tutorial) can be found in the EFS – Encrypting File System folder at the following URL:

  https://collaborationportal.dadeschools.net/departments/9412/itsdocs/

Policy

I. Management is responsible for:

A. Knowing the assets and services for which they are responsible and applicable control requirements.

B. Authorizing users to utilize information assets and ensuring all equipment is used for School Board approved purposes only.

C. Assigning custodial authority and responsibility.

D. Ensuring effective use of control facilities.

E. Responding in a timely and effective way to loss or misuse of information assets.

Policy (continued)

II. The owner is the manager or management representative who is responsible for working and communicating judgments and decisions on behalf of the School Board for identification, classification, and protection of the school system's information assets. Ownership conveys authority and responsibility for:

A. Classifying the assets, authorizing access, and assigning custody.

B. Ensuring that information asset security and application system controls are effective and in place.

C. Communicating control and protection requirements to users and custodians.

D. Reporting security violation attempts to management.

III. A user is an individual authorized to utilize information assets and services. A user is responsible for:

A. Complying with information asset security and application system controls as specified by the owner and custodian.

B. Using the School Board's information processing assets only when authorized by management and only for approved purposes.

C. Ensuring that system, data, and application passwords meet specified requirements, are not shared, and are properly protected.

D. Effectively using control facilities and capabilities.

E. Reporting security violation attempts to management.

Policy (continued)

IV. A custodian is a provider of information processing services to others and/or to himself in support of School Board activities. A custodian is responsible for:

A. Administering owner-specified information asset security and application system controls for information and information processing assets in his custody.

B. Within the School Board's implementation of their application system controls, programmers are provided with emergency authority to access files *only* when required for the support of production. Every update to a production file made by someone with the emergency authority is logged on a RACF Production Update Report. A specific custodial responsibility is the daily review of this report by the system supervisor to ensure that these updates are justified.

C. Administration of access to information assets.

D. Providing and administering physical and procedural safeguards for protection of information assets.

E. Effectively communicating installation control facilities, rules and restrictions to owners and users.

F. Providing for timely detection and effective response to unauthorized attempts to gain access to data or restricted areas.

G. Reporting security violation attempts to management.