

**SUBJECT:      REMOTE ACCESS**

**Supersedes:**    None; New policy

**Effective:**     February 15, 2005

**Page:**          1 of 3

**1.0    POLICY PURPOSE**

Due to the nature of your job functions at Detroit Public Schools (DPS) along with a “need to know” requirement to complete the functions, you were granted DPS remote access via Cisco Appliance - Virtual Private Network. The purpose of this policy is to define standards for connecting to the DPS network from various hosts. These standards are designed to minimize the potential exposure to DPS from damages that may result from unauthorized use of DPS resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to district image, along with damage to internal information technology systems.

**2.0    SCOPE**

This policy applies to all DPS employees, contractors, vendors, and agents with a DPS-owned or personally-owned computer or workstation used to connect to the DPS network. This policy applies to remote access connections used to do work on system support, modifications, or enhancements when required.

**3.0    POLICY**

It is the responsibility of DPS employees, contractors, vendors, and agents with remote access privileges to the DPS district network to ensure that their remote access connection is given the same consideration as the user's on-site connection to DPS.

Any unauthorized connections to or from the DPS network with outside organizations or individuals may potentially jeopardize the DPS network and infrastructure security. Starting points of connections include the Internet, DPS customers, business partners, or any personal locations. The district security and network groups reserve the right to audit compliance with this policy.

**3.1    REMOTE ACCESS ACCOUNTS WILL BE DELETED UNDER THE FOLLOWING CIRCUMSTANCES**

- The employee appears on the Human Resources “terminated list”
- The person’s manager submits a request to have the account removed
- The account has not been used in the past 90 days

**3.2    ACCESS TO DPS RESOURCES**

Access security controls will be implemented upon the principle of least possible privilege. Users are given the minimum access necessary to perform their jobs. Remote access denies access to all DPS resources by default. Access to a server is only given after proper authorization has been received. Access to DPS

servers is controlled via groups called “tunnels”. At no time should the user disclose his or her login or password to anyone, not even family members.

### **3.3 DPS ANTIVIRUS POLICY**

All corporate and privately owned computers, laptops, servers, or other devices that connect to the DPS network will run corporate approved antivirus software and apply update files to the software as directed.

### **3.4 ADDITIONAL GUIDELINES**

Users granted DPS remote access should refer to the following policies for guidelines on protecting information and maintaining system security when remotely accessing the DPS network:

- a. Policy 13.04 - Information Classification
- b. Policy 13.05 - Password Protection

### **3.5 USE OF NON DPS OWNED EQUIPMENT**

DPS will allow district employees to gain access to the district network and resources while using non-DPS owned equipment with the following conditions and understanding:

- DPS has the right to install or delete files or programs on user owned equipment it deems necessary for the protection and security of DPS network and assets contained within
- When remotely accessing the DPS network you must ensure that your own personal computer is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user
- You must comply with DPS antivirus standards
- By downloading and/or installing any DPS software, you acknowledge and agree to the following:
  - DPS shall not be liable for any interference with the operation and/or performance of your personal computer and/or any loss of data which results from installing any DPS software
  - Any DPS software, which is downloaded and/or installed, has been provided for use in connection with your employment at DPS. Under no circumstances should any DPS software be copied or distributed to any other person
  - The DPS software you use for DPS business must be immediately removed from your personal computer and promptly returned to DPS if your employment with DPS is terminated.
  - If you should transfer positions within DPS you are to remove any software you no longer require to perform the duties of your position.

## **4.0 ISSUANCE OF REGULATIONS/STANDARD OPERATING PROCEDURES**

The Chief Technology and Information Systems Officer is authorized to develop regulations and/or standard operating procedures to implement this policy.

**5.0 FAILURE TO COMPLY**

Failure to comply with this policy or the corresponding regulation may result in a recommendation to the Chief Executive Officer for appropriate disciplinary action.

**6.0 AGREEMENT**

I, \_\_\_\_\_ (print name) have read the Detroit Public Schools Remote Access policy, dated \_\_\_\_\_. I understand it and agree to abide by it.

\_\_\_\_\_  
Signed

**Attachments:** Technology Specifications

**See also:** Policy 13.04 - Information Classification  
Policy 13.05 - Password Protection

**Legal References:** None

**Labor Contract References:** None

## **TECHNOLOGY SPECIFICATIONS**

The secure connection you are applying for is called a tunnel. The VPN concentrator located in the district data center uses tunneling protocols to negotiate security parameters, along with creating and managing tunnels. The VPN concentrator functions as a bidirectional tunnel endpoint; it can receive plain packets, encapsulate them, and send them to the other end of the tunnel. The packets are unencapsulated and sent to their final destination.

The VPN concentrator performs the following functions:

- Establishes tunnels
- Negotiates tunnel parameters
- Authenticates users
- Assigns user addresses
- Encrypts and decrypts data
- Manages security keys
- Manages data transfer across the tunnel

The Cisco Appliance - VPN should install and run on most personal home computers. You will receive an Installation and Configuration guide following your remote access approval. You should always back-up your computer before making any changes or attempting to install new software. Through a combination of signing the application for remote access you are agreeing to the policies covered in the next session. If you are using a district issued laptop or computer, Network Services will configure your machine for remote access. Following is the standard configuration:

### **A. Operating System**

- Window 95/98
- Windows NT/2000
- Windows XP Pro

### **B. Hardware**

- Pentium 300 or higher
- 64 Mb Ram or higher
- CD Rom Drive
- 50 Mb free disk space
- 28.8 modem installed and configured (minimum)
- Most Cable modem implementations are supported

### **C. Other Software**

- Mail Client, Outlook 98 or higher
- Microsoft Internet Explorer 6.0 or higher

Due to numerous technical issues Network Services cannot guarantee that you will be able to connect to DPS resources when using non-standard hardware or software. Problems may arise based on the following conditions:

- A non-DPS standard router or firewall
- When DSL is the Internet connection
- You have a home network

If you are unable to get your home system to connect to Cisco Appliance - VPN, and it is necessary for you to connect to the DPS network, then you and your manager will need to discuss other possible solutions using DPS hardware and software.