

SUBJECT: **VENDOR ACCESS**

Supersedes: None; New policy

Effective: February 15, 2005

Page: 1 of 1

1.0 POLICY PURPOSE

The purpose of this Vendor Access policy is to create an environment within Detroit Public Schools (DPS) that maintains system security and availability, data integrity, and individual privacy by preventing unauthorized access to information and information systems and by preventing misuse of, damage to, or loss of data. Information is a Detroit Public Schools asset. When business partners remotely enter the DPS network continued assurance is necessary to protect information commensurate with its value, criticality, and sensitivity.

2.0 SCOPE

Vendors play an important role in the support of hardware and software management and operations for their customers. Remote access would allow for correction of software and operational system problems. Vendors could monitor and fine-tune system performance; they could monitor hardware performance and errors; they can modify environmental systems; and they could reset alarm thresholds if necessary. DPS is responsible for setting limits and controls of what can be seen, copied, modified, and controlled by vendors.

3.0 VENDOR RESPONSIBILITY

- Vendors may not enter the DPS network for the purpose of solicitation or sales to DPS employees or students.
- Remote access to DPS networks cannot be used for advertisement purposes.
- Any knowledge gained in working with DPS network components cannot be used for commercial or personal purposes.
- Vendor employees accessing the DPS network must have a signed "confidentiality agreement" on file with the DPS Network Manager.
- Vendor employees accessing the DPS network must adhere to this policy and DPS Policy 13.03 - Information Security
- Vendors remotely accessing the DPS network must have approved and up-to-date antivirus software.
- Vendors may not use the DPS network for gaining access to the Internet.
- Vendors shall notify the DPS Network Manager when an employee, who has access to the DPS network, leaves the vendor or is transferred to another position that no longer requires access.
- Vendors shall assume all responsibility for protection of their private network(s) that may be remotely connected to the DPS network.
- Only employees of the vendor who have approved access shall use the resources accessible via the vendor remote connection to the DPS network. No sharing of accounts on the DPS network will be permitted.

- The vendor shall notify the DPS Network Manager whenever there is a change in personnel performing work over the DPS network.
- Vendor employees accessing the DPS network will be asked to attend a brief (1/2 hour) awareness or training session. A Computer Based or Web Based Training program may be substituted in lieu of a face-to-face session.

4.0 NETWORK MANAGER RESPONSIBILITY

- DPS Network Manager is responsible for determining the “need to know” requirements for vendors requesting remote access to the DPS network.
- In general, services provided vendors through remote access to the DPS network should be limited only to those services needed, and only to those devices (hosts, routers, etc.) needed. Blanket access shall not be provided to anyone. The default position will be to deny all access and then only allow those specific services that are needed. In no case shall the vendor remote access connection to the DPS network be used as the Internet connection for the vendor.
- DPS Network Manager is responsible for building the technology necessary for vendor remote access.
- DPS Network Manager or designee will issue the initial remote access password. He/she will ensure that all connecting vendors adhere to DPS Policy 13.05 - Password Protection
- DPS Network Manager or designee will approve vendor anti-virus software.
- Working with the Data Security Coordinator the DPS Network Manager will have “confidentiality agreements” for all vendor personnel accessing the DPS network.
- Vendor shall contact DPS Network Manager or designee prior to accessing the DPS Network.
- Using tracking capabilities or log files the DPS Network Manager or designee will track all vendor activities while being remotely connected to the DPS network.
- At no time, should the DPS Network Manager rely on access/authorization control mechanisms at the vendor site to protect or prohibit access to DPS’ confidential information

5.0 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.

6.0 FAILURE TO COMPLY

The DPS Network Manager and his/her designee are responsible for understanding and complying with the DPS Vendor Access policy. Non-compliant situations will be brought to the attention of the DPS Information Security Manager and Chief Technology and Information Systems Officer. Additionally, vendor management will be made aware of non-compliance with this policy. Depending on the severity, individuals who violate this policy will receive the following:

6.1 Vendor Non-Compliance

- Change of vendor personnel who can access DPS network remotely
- Loss of remote access capabilities

- Termination of contract with DPS
- Criminal or civil prosecution

6.2 DPS Non-Compliance (Network Manager and designees)

- Loss of network connectivity
- Subjected to DPS disciplinary process including dismissal
- Criminal or civil prosecution

7.0 AGREEMENT

I, _____ (print name) have read the Detroit Public Schools Vendor Access policy, dated _____. I will access the DPS network in accordance with the requirements set forth herein. I acknowledge that misuse of any access privilege will result in appropriate disciplinary action being taken.

Signature

Attachments: None

See also: None

Legal References: None

Labor Contract References: None