

SUBJECT: ENTERPRISE WIRELESS

Supersedes: None; New policy

Effective: February 15, 2005

Page: 1 of 2

1.0 POLICY PURPOSE

Detroit Public Schools (DPS) is committed to protecting information and information systems confidentiality, authentication, availability, integrity, and non-repudiation independent of technology being used. The goals are further explained as follows:

- **Confidentiality:** Verify that information is private and seen and accessed only by intended recipients. Confidentiality in wireless is created via access control and encryption.
- **Integrity:** Verify that information received is the same information transmitted by the originator, unchanged.
- **Authentication:** Identify an individual or computer to ensure access to information is authorized. Access control/account administration is imperative in a wireless environment.
- **Non-repudiation:** Ensure that an individual cannot deny sending or receiving information.
- **Availability:** Ensure that information and supporting service resources are up and running when needed.

To best obtain the above goals it is imperative the following objectives are met:

- Protect DPS information, users, and wireless devices from unauthorized disclosure.
- Ensure that DPS information is protected against an intrusion that could alter, disable, or circumvent the transmission.
- Require centralized oversight, configuration management, and control of wireless devices.
- Ensure protection against physical compromise.
- Ensure there will be no adverse impact to DPS critical operations if wireless computing devices are rendered inoperable.

2.0 SCOPE

1. Administrative Offices – all DPS business units
2. Schools – employees working within a DPS school or technical centers
3. DPS Wireless – Network is wireless telecommunications or computer related equipment or interconnected systems or sub-systems of equipment that is used in the DPS administrative offices or schools to support DPS business, operations, and missions in the acquisition, storage, management, movement, control, display interchange, transmission, or reception of data

3.0 POLICY

All DPS Wireless – Network users will:

- Obtain business unit management approval prior to use of DPS Wireless – Network.
- Use equipment registered, approved, acquired, certified and accredited by DPS Technology and Information Systems (TIS) Network Manager
 - DPS TIS Network Management is building a 802.11b wireless network
 - DPS TIS Network Management is building a standardized (hardware) network
- Comply with:
 - Policy 13.03 - DPS Information Security
 - Administrative Regulation 13.03 - DPS Information Security
 - Policy 13.05 - Password Protection
 - Policy 13.06 - Remote Access
 - Policy 13.07 - Electronic Mail (Email)
 - Enterprise Wireless Policy and Administrative Regulation (this document)
- Attend training on use of the DPS Wireless – Network
- Report loss or stolen DPS Wireless – Network components to the DPS TIS Network Manager by the next business day
- Report violation of policy through chain of command

4.0 ISSUANCE OF REGULATIONS/STANDARD OPERATING PROCEDURES

The Chief Technology and Information Systems Officer (CTIO) has developed regulations and/or standard operating procedures to implement this policy.

5.0 FAILURE TO COMPLY

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

6.0 EXCEPTIONS

Any exceptions to this policy must be documented and approved by the DPS Chief Technology and Information Systems Officer. The DPS TIS Network Manager will monitor actions that will create exceptions.

7.0 AGREEMENT

I, _____ (print name) have read the Detroit Public Schools Wireless policy, dated _____. I understand it and agree to abide by it.

Signature

Attachments: Administrative Regulation 13.02 – Enterprise Wireless

See also: None

Legal References: None

Labor Contract References: None

DETROIT PUBLIC SCHOOLS
ADMINISTRATIVE REGULATION

ENTERPRISE WIRELESS

This Administrative Regulation implements Detroit Public Schools (DPS) Policy 13.02 – Enterprise Wireless

1.0 DPS Wireless – Network required security features are:

1. Password protection or strong identification and authentication techniques such as Public Key Infrastructure (PKI) or biometrics for those using DPS Wireless - Network that store, process, and transmit DPS information.
2. Features and capabilities to disable InfraRed, Radio Frequency, and microphone/audio
3. Encryption via NIST FIPS approved or NSA-approved encryption mechanism (128 byte) while in the wireless environment
4. Compliant with any DPS policies for authentication
5. DPS standard virus protection software or equivalent protection
6. Intrusion detection, auditing, and monitoring mechanisms

2.0 DPS Wireless – Network common Technology and Information Systems (TIS) transport infrastructure deployed within the Fisher Campus

1. Be under the direct control of the DPS TIS Network Manager
2. Filtering of Media Access Control (MAC) addresses
3. Provide the capability to restrict user options to minimize the amount of traffic related information transmitted
4. Provide security mechanisms that are scalable, manageable, flexible, and standards based
5. Employ security mechanisms that are compatible and inter-operable with those mechanisms used on wired voice and data telecommunications networks and computing devices
6. Support strong identification, authentication, and auditing if remote administration is employed

3.0 DPS TIS network management responsibilities:

1. Provide oversight for administrative offices and schools wireless policies and implementations
2. Provide guidance for all wireless risk assessments. Includes identifying vulnerabilities, threats, present controls, and potential controls required to mitigate risks
3. Provide security awareness training
4. Provide documentation and recommendations to the DPS Chief Technology and Information Systems Officer (CTIO) that a business unit or individuals be disconnected from the DPS common TIS transport infrastructure for repeat violations

5. Request or conduct an annual audit to detect unauthorized DPS - Wireless Network uses within the administrative offices. This would include production use and development projects by TIS intended on improving DPS wireless network.
6. Report security related events to DPS/CTIO
7. Develop recovery and restoration guidance
8. No other departments may deploy 802.11 or related wireless standards access points without prior approval and coordination with DPS TIS network management