PURPOSE
The purpose of this policy is to define connection to the District's network through wireless networking. These standards are designed to minimize the potential exposure of the District from damages which may result from unauthorized use of District resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical District internal systems, etc.

SCOPE
This policy applies to all District employees, contractors, vendors and agents with a District issued computer and other equipment used to connect to the District network.

BACKGROUND
With the Institute of Electrical and Electronics Engineers (IEEE) ratification of the 802.11b standard for wireless networking in 1999 and the subsequent proliferation of interoperable, affordable products that support that standard, wireless LAN technology (WLAN) has established itself as an important complement to the traditional wired data network because of the mobility they provide. 802.11b WLAN technology is also beneficial for gaining network access in locations that are difficult, expensive, or inconvenient to wire. Examples include outdoor areas, conference rooms, rooms with solid walls (to avoid running cables in unattractive surface-mounted conduit), and structures with asbestos, and historical buildings with strict regulations governing modifications. Despite these advantages, 802.11b WLANs have their limitations. For example, they are an order of magnitude slower than wired LANs. Despite claims of 11 Megabits per second (Mbps) of bandwidth, the practical limit is about 5 Mbps -- and that's shared among all people using that Access Point. Consequently, it is not hard for one person to monopolize the bandwidth of an Access Point and kill the performance for the other people using it. Compare that to a typical wired, switched network connection on the District campus that is dedicated to one computer and operates at 100 Mbps in full duplex (i.e., you get nearly the full 100 Mbps in both directions -- incoming and outgoing data traffic).
WLANs are also inherently insecure. Tools are readily available to capture data packets from the airwaves and thereby "snoop" on someone else's communications. Consequently, wireless users must take extra precautions and adhere to standards to ensure secure communications over a WLAN.

POLICY

Technology
1. Only the IEEE 802.11b and/or 802.11a standard for wireless LANs is allowed.
2. All Access Points will be Cisco products. No other vendor or model of Access Points will be permitted on the District network.
3. For PC cards, the Cisco Aironet 350 Series Client Adapter (or a newer model) that supports 128-bit WEP encryption is strongly recommended.
4. Only the IP protocol will be supported.
5. The District Systems Administrators or designees are responsible for updates to the technology standards as the industry and technology change.

**Installation and Management**
1. District Technical Support will be the sole provider of design, specification, installation, operation, maintenance, and management services for all Wireless Access Points.
2. All IP addresses for the District WLAN will assigned by a Dynamic Host Configuration Protocol (DHCP) service maintained by District Technical Support.
3. Installation must comply with all health, safety, building, and fire codes.

**Radio Signal Interference**
1. 802.11b WLANs operate in the unlicensed 2.4 GHz range and conform to the IEEE 802.11 DSSS (Direct Sequence Spread Spectrum) specification. Other wireless devices use the same 2.4 GHz frequency band and may disrupt the operation of the District Spectrum) specification. Other wireless devices use the same 2.4 GHz frequency band and may disrupt the operation of the District wireless network. These include cordless phones, microwave ovens, cameras, keyboards, mice, audio speakers, and other wireless LAN devices like earlier versions of 802.11. To assure the highest level of service to WLAN clients, the use of all other 2.4 and 5 GHz devices should be is discouraged on the District campus.
2. If interference occurs, the 802.11 network will have priority. In cases of significant problems, users of other devices will be required to cease using those devices. It is recommended that, when practical, people purchase devices operating at other frequencies (e.g., 900 MHz) to avoid this possibility.
3. The District System Administrators have the authority to require cessation of unauthorized use of the 2.4 and 5 GHz bands.

**DEFINITIONS**

**802.11b**: An IEEE standard for wireless data networking rated at 11 Megabits per second throughput operating in the FCC unlicensed 2.4 GHz Industrial/Scientific/Medical (ISM) band and using Direct Sequence Spread Spectrum (DSSS) technology to transmit the signal. The range of the signal indoors is up to 150 feet at 11 Mbps (300 feet diameter), or 800 feet outdoors. The range and strength of the signal are reduced significantly as it passes through walls, floors, and other physical structures.

**802.11a**: An IEEE wireless network standard currently under development that increases the bandwidth to 54 Mbps per Access Point, but decreases the range of the signal to about 35 feet indoors. It operates in the 5 GHz unlicensed National Information Infrastructure (U-NII) frequency range.

**Access Point**: A hardware device that serves as a communications "hub" for wireless clients and provides a connection to the wired LAN.

**Bluetooth**: An IEEE wireless networking standard (802.15.2) operating in the 2.4-GHz frequency band designed for lower power and shorter range (less than 30 feet) than 802.11b,
hence its label as a "personal area network" wireless technology (WPAN). It's designed to replace cables that connect devices, such as a Personal Digital Assistant (PDA) to a desktop computer, rather than functioning as an extension to a wired network like 802.11 wireless networks. Bluetooth uses a spread spectrum, frequency hopping, full-duplex signal at up to 1600 hops/sec.

SSID: The "Service Set Identifier" may be used as a relatively insecure security key for a WLAN, somewhat like a password. If the SSID is set in the Access Point, then only client wireless cards configured with the same SSID may connect to that Access Point.

WEP: "Wired Equivalent Privacy" that provides limited security to a wireless connection by encrypting all data transmitted between the computer and the Access Point. At this time, 40-bit and 128-bit WEP is available on most vendors' Access Points, and District supports both.

Wireless PC Card: Hardware device in a client computer (most often a card that fits in a Personal Computer Memory Card International Association (PCMCIA) Type II slot in a notebook computer) that communicates with an Access Point via radio signals (i.e., without wires). Also known as "wireless client adapter".

WLAN: "Wireless Local Area Network". The term often used for a wireless network within a limited area consisting of one or more wireless Access Points that provide network connectivity to computers equipped with wireless capability (usually a notebook computer with a wireless PC card). In essence, a WLAN provides the functionality of a wired LAN without the physical constraints of the wire.

ENFORCEMENT

Use of non-District/personal devices such as tablet, laptop, cellphone, etc. as Wireless Access Points for network access, including Remote Access, is not permitted at any time.

If a wireless using employee comes to a District office to work, the employee will use an Ethernet cord for connectivity to the District network.

Any employee found to have violated this policy may be subject to disciplinary action immediately, up to and including termination of employment.