

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	04-02				
State of Rhode Island Department of Administration Division of Information Technology		TITLE	Wireless Network Devices		

## 1. Overview

The intention of this policy is to define roles and responsibilities for the design of any new wireless network, the installation, registration and management of wireless access points, management and allocation of the wireless frequency spectrum and the services offered to end users for wireless access.

## 2. Scope

This policy applies to all wireless network devices utilizing the Division of Information Technology's IP space including private non-routable IP space within the State's networks.

Division of Information Technology (DoIT) is responsible for the operation and management of State's network infrastructure. A natural extension to the fixed network currently in existence is a wireless network. In order to ensure reliability, integrity, interoperability and security between the wired and wireless domains it is the responsibility of DoIT to ensure the design, management and appropriate use of the State's wireless infrastructure is in accordance with best practice and existing policies.

## 3. Definitions

Wireless networking is a relatively new technology so some definitions will aid in clarification of the policy.

- **Wireless Network:** The network technology that uses radio frequency spectrum to connect computing devices to a wired port on the State network. Common technologies are IEEE 802.11a, 802.11b and 802.11g. Bluetooth is a similar technology.
- **Wireless Infrastructure:** The wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless network
- **Base Station:** A network device that serves as a common connection point for devices in a wireless network. Access points use wireless antennas instead of wired ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and are usually connected to the wired network.
- **Access point:** Same as **Base Station**.
- **Coverage:** The physical area where a level of wireless connectivity is available.
- **Channel:** The chosen frequency for communication between the end point and the base station.

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	04-02				
<b>State of Rhode Island Department of Administration Division of Information Technology</b>	TITLE	<b>Wireless Network Devices</b>			

- **RF Interference:** The degradation of a wireless communication signal caused by electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.
- **Security:** The condition that provides for the confidentiality of data transmitted over a wireless network.
- **SSID:** Service Set Identifier, essentially a name that identifies a wireless network. All devices on a specific wireless network must know the SSID of that network.
- **Client hardware/software:** The equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device.

#### 4. Objective

There are three major risks with an ongoing ad-hock deployment of wireless networks in the state network.

- I. **Security:** By their very nature wireless LANs are open to anyone within range of the access point. Physical boundaries are no longer relevant. If a wireless access point is connected to the campus network without restrictions anyone with the proper equipment will be able to access the network. Furthermore, anyone with the proper equipment can spy on traffic. They can see users' passwords as well as other data. In line with other policies, security of wireless installations has to be rigorously managed.
- II. **RF Interference:** There is a finite amount of bandwidth available for wireless use. The most common wireless LAN technology (802.11b) defines only 3 (or possibly 4) channels for effective use. If wireless LANs are installed without coordination with others in the area, interference is likely. This may result in significantly degraded performance for everyone.
- III. **Equipment Diversity:** All standards compliant wireless equipment from reputable manufacturers will coexist with each other even leaving aside possible interpretations in the standard. However for a campus wide wireless LAN infrastructure to be properly planned, implemented and managed, appropriate hardware needs to be chosen for deployment. Low cost 'consumer-oriented' devices which do not provide the management capabilities for campus wide networks should be avoided in favor of more appropriate equipment.

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	04-02				
<b>State of Rhode Island Department of Administration Division of Information Technology</b>	TITLE	Wireless Network Devices			

The objective of this policy is to define a framework where DoIT works with departments and facilities to enable the deployment and ongoing management of a wireless network infrastructure. The intention is not to restrict or constrain the growth of the network.

DoIT shall act as overall coordinators and controllers of the network. Individual departments and Agency IT Managers within those departments shall, where appropriate, be responsible for the localized management and implementation of the access points and infrastructure.

## 5. Policy

**5.1** Wireless base stations must abide by all national regulations pertaining to wireless devices. Furthermore, wireless technologies must conform to DoIT standards. Individuals and departments are expected to purchase in line with State purchasing policy and by seeking guidance from DoIT.

**5.2** No wireless base stations are allowed to be connected to the state network without an approved Request for Change.

**5.3** Agencies must appoint a point of contact for all wireless access points, and must notify DoIT network services. The point of contact will advocate for the department and act as an official representative.

**5.4** Allocation of channels, SSID and encryption standards must be authorized by network services before deployment.

**5.5** ALL wireless LAN communications must be encrypted.

**5.6** All wireless communication shall require user authentication before granting access to department network and beyond.

**5.7** Wireless networks must be designed and deployed to avoid any interference between competing devices in the electro magnetic spectrum. Other devices may mean neighboring wireless base stations or other components using the radio spectrum such as cordless telephones or competing technologies. In the event that a wireless device interferes with other equipment the local department is expected to resolve the situation. Disputes over channel allocation should be handled by the official point of contact for that base station. Where multiple units or departments are involved Network Services will act as arbiter or coordinator.

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	04-02				
<b>State of Rhode Island Department of Administration Division of Information Technology</b>		TITLE	Wireless Network Devices		

5.8 Physical security is considered the responsibility of the department when planning the location of wireless access point and other wireless network components. DoIT security personnel will review and approve Requests for Change for new wireless network devices.

## 6. Conformance with Existing Policies

DoIT is authorized to take whatever reasonable steps are necessary to ensure compliance with policies designed to protect the integrity and security of the state network.

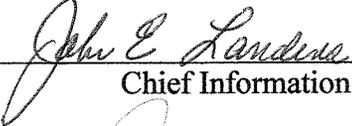
Due to the nature of wireless networks the following should also be noted:

**Authorization to disconnect** any wireless network on state network which poses a security threat.

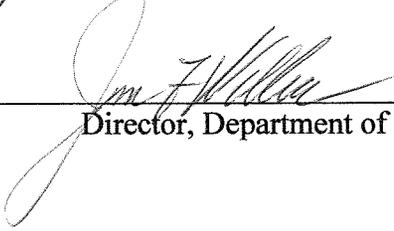
If a serious security breach is suspected or in process DoIT may disconnect wireless devices immediately. Every reasonable attempt will be made beforehand to reach the registered 'point of contact' to resolve security problems. Network Services shall also have the authority to disconnect any wireless network from the network whose traffic patterns seem unusually suspicious or violates practices set forth in this and other policies.

It is the responsibility of the department, agency, or unit to be knowledgeable regarding the provision all DoIT policies.

## 7. APPROVALS

  
 \_\_\_\_\_  
 Chief Information Officer

7/20/2008  
 \_\_\_\_\_  
 Date

  
 \_\_\_\_\_  
 Director, Department of Administration

8/1/08  
 \_\_\_\_\_  
 Date