NEW JERSEY CITY UNIVERSITY

Section Number ____________ Section Header: __________________________

Subject: __Wireless Networking Policy________________________ Effective Date: _May 2005_______

Responsible Office: _Department of Information Technology__ Responsible Officer: ________________

TABLE OF CONTENTS

INTRODUCTION

The Department of Information Technology (DoIT) began implementation of wireless LAN technology as an extension of the University's data network summer 2004. The Wireless LAN is not a replacement to the existing university hard-wired network but a supplement to it. Wireless service is available in most areas where people tend to congregate, including to the main campus center court, GSUB cafeteria, and other locations.

PURPOSE

Although wireless technology is a common means of connecting to a network and the devices readily available at commodity pricing, simply plugging such hardware into the University network without proper configuration presents a potential service problem and serious security risk for the entire campus community. Unauthorized wireless access points will conflict with the university wireless service. The standard Wireless Encryption Protocol (WEP) used by these devices provides only limited protection and the proliferation of wireless sniffers gives unauthorized intruders an easy means of testing and breaking these simple security features.

To avoid potential conflicts, site surveys are critical to the success of the wireless infrastructure. In addition, measures must be taken to ensure that wireless LAN access is limited to authenticated NJCU faculty, staff and students, and to secure data through high-level encryption while being transmitted. Further, a single vendor solution for access points is the only way to provide seamless roaming over the wireless infrastructure. It is therefore imperative that all requests for wireless service go through THE DOIT. Further, it is critical to develop policy, procedures and guidelines that assure the safety and integrity of the University's wireless network in the future.

SCOPE

This document applies to all members of the university community, including third party vendors, contractors and consultants.

DEFINITIONS

Wireless Network – A wireless-based data network. The University's wireless network uses the current standard wireless protocols, 802.11b and 802.11g.

Wireless Protocol – The transport specification that provides the interface for wireless communications. There are several protocols in use today. The most common are 802.11b and 802.11g. A new protocol, 802.11n, is currently being ratified and will most likely replace both b and g protocols over time.

Wireless Adapter – A device that provides connectivity to a wireless network. This device is commonly built into laptop computers but can be added as a PC-Card peripheral.

Access Point – A device that provided the wireless service. Several are needed to provide service to any given area, depending on the coverage area desired. Access points are physically connected to the wired network, which provides the interconnectivity to other network resources.

POLICY

Access

- Access is provided through network authentication using a login and password.
- All members of the University community may use the wireless network, provided they have a valid GothicNet account.

- University visitors can be provided limited access to the wireless network by applying for guest access. Guest access requires sponsorship and authentication. The guest access form is available from the DoIT website, support page, GothicAir section.
- All wireless adapters must conform to the University's Wireless Network Standards. These standards are available from the internal Technology Standards & Services website.
- Use of the University Wireless Network shall be subject to the University Computer Usage Policy and Guidelines.
- Unauthorized persons attempting to compromise the University's wireless network or interfere with the University's wireless airspace will be prosecuted to the full extent of the law.

Connectivity

- Installation, engineering, maintenance, and operation of the wireless network and access points on any property owned or tenanted by the University are the sole responsibility of the DoIT.
- The DoIT will extend the university network to provide wireless service to any area based on the application need, demand and funding.
- The installation of any device that interferes with authorized wireless transmissions is strictly prohibited. (see the Potential Interfering Devices section, below)
- Installation of Access Points by individuals or departments is prohibited.
- Due to interference, wireless 2.4 GHz telephones and other 2.4 GHz devices will are not permitted in areas of wireless technologies.
- Unauthorized wireless connections to the university network will be terminated.
- All wireless Access Points must conform to the University's Wireless Network Standards.

KEY PERFORMANCE INDICATORS

The following success of the policy will be assessed annually using the following quantifiable measures:

1. There is no interference from rogue APs
2. All supplemental APs are known and accounted for

PROCEDURES

Accessing the wireless network

- Please refer to the GothicAir User Guide, which can be found on the DoIT website, support page, GothicAir section.

Requesting access point installations

- Fill out the Wireless Service Request Form. This form can be filled out online and submitted electronically or a hardcopy can be downloaded from the DoIT website, Support page, GothicAir section and submitted to the Help Desk, Rossey Hall, Room 58.
- A DoIT network administrator will contact you for additional information and set up or supervise installation.
- Installation may require the services of an outside contractor. Charges may be assumed by the requestor depending on budget constraints and the complexity of installation.

As requirements and usage patterns change, it may be necessary to resurvey the wireless coverage areas. This is a necessity in order to provide the appropriate level of service and maintain seamless roaming between wireless cells.

Potential Interfering Devices

There are many devices that utilize the 2.4 GHz radio frequency and new devices are released regularly. The following is a sample list of devices that are known to cause interference with wireless networks. In some cases, simply moving the device may clear the interference. If moving the device does not clear the interference, it must be removed from operation.

- Microwave ovens operating within approximately 10 feet an Access Point
- 2.4 GHz Wireless Telephones
- 2.4 GHz Wireless Speakers
- Rogue Access Points and computers acting as Access Points

The DoIT may be contacted to help determine if a device utilizes the 2.4 GHz frequency and if it will cause interference. It is hoped that all faculty, staff, and students will abide by the airspace policies & procedures set forth in this document which will help in providing the best wireless network service possible.

RELATED DOCUMENTS

- GothicAir User Guide
- Outdoor Wireless Coverage
- Indoor Wireless Locations
- Wireless Security Recommendations

- Hints for Wireless Road Warriors

FORMS

- GothicAir Guest Access Form
- Wireless Service Request Form

All documents and forms are available from the DoIT website, Documents page and the University Policy website page.

RESPONSIBLE PERSONNEL

Responsibility	Title	Department	Telephone	Fax	Email
AP Installation	Helpdesk	DoIT	Ext. "HELP"		helpdesk@njcu.edu