FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

University Wireless Network Infrastructure # 1910.010

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
April 6, 2009	May 20, 2024	Division of Information Technology

POLICY STATEMENT

The deployment and management of wireless access points in all buildings of Florida International University, including common areas of the campus, are the responsibility of the Division of Information Technology.

Interference, disruption, or unauthorized interception of wireless networking traffic is a violation of this policy. All equipment that operates in the radio frequency spectrum must be installed, configured and monitored to avoid physical and logical interference between components of different network segments and other equipment. In the event that a wireless device interferes with other
equipment, the university shall resolve the interference as deemed necessary.

Only Division of IT approved hardware and software can be used to provide wireless access to the FIU core network and to the Internet.

Wireless access points must meet all applicable rules of regulatory agencies including, without limitation, rules from the:

- Federal Communications Commission
- Public Communications Commission
- Health, building and fire codes

SCOPE

This policy applies to all faculty, staff, students, POI, and guests.

REASON FOR POLICY

This policy governs the deployment, maintenance, standards, and use of the FIU Wireless Electronic Communications Resources. This document also addresses resolution of interference issues that might arise during use of specific frequencies.

DEFINITIONS	
TERM	**DEFINITIONS**
IEEE 802.11i	Refers to an amendment to the original Institute of Electrical and Electronics Engineers Wireless 802.11 standard specifying security mechanisms for wireless networks that include encryption and authentication.
Access Point	Any piece of equipment that allows wireless communication using transmitters and receivers to communicate. These devices act as hubs and allow communications to the campus network.
Interference	Interference is the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Such interference can either slow down a wireless transmission or completely eliminate it depending on the strength of the signal.
Privacy	Privacy is the condition that is achieved when successfully maintaining the confidentiality of personal, student and/or employee information transmitted over a wireless network.
Wireless Infrastructure	Wireless infrastructure refers to wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless network infrastructure

ROLES AND RESPONSIBILITIES

The Division of Information Technology is responsible for providing wireless services to the university community as defined in the scope of this policy.

Division of Information Technology:

- Creating, maintaining, and updating wireless infrastructure policy standards.
- Creating, maintaining, and updating wireless infrastructure network security policies.
- Creating, maintaining and updating wireless communication network security policies.
- Maintaining a database of all wireless networks and access points on campus.
- Creating, maintaining and updating wireless infrastructure security standards.
- Resolving wireless communication interference problems.
- Managing and deploying wireless infrastructure systems for the University.
- Informing wireless users of security and privacy policies and procedures related to the use of the wireless infrastructure.
- Monitoring performance and security of all wireless networks within FIU and maintaining network statistics as required to prevent unauthorized access to the campus network.
- Monitoring the development of wireless network technologies, evaluating wireless network technology enhancements and,

as appropriate, incorporating new wireless network technologies within FIU.
• Disabling access points not installed by the Division of Information Technology.

University Community (Faculty, Staff, Students, POI, Guests):
• Adhering to the Wireless Network Infrastructure Policy.
• Informing wireless users of security and privacy policies and procedures related to the use of wireless communications.

IT Security Office:
The IT Security Office (ITSO) has the responsibility to evaluate the seriousness and immediacy of any threat to campus information system resources or to the Internet and to take action to mitigate that threat. Any action taken will be based on the risk associated with the threat and will take into account, to the extent possible, its potential negative impact to the University's mission that may because by making the offending computer(s) inaccessible.

The ITSO is also responsible for the following:
• Random monitoring of the wireless network for transmission of sensitive information.
• Perform random audits on systems connected to the wireless network to verify system and anti-virus updates.
• Evaluate and mitigate threats to the FIU Network or the Internet.

RELATED RESOURCES

This section within the policy should align operations. Links to other policies, laws, forms, tools, and processes suggested to support the implementation or required for compliance with the policy. Examples include:

- Links to federal state or local laws or relations

Background material that is helpful and not directly related to policy implementation

CONTACTS

Division of Information Technology
Network Management Services
11200 SW 8 ST,
Miami, FL 33199
305-348-2284
It.fiu.edu

HISTORY

Initial Effective Date: April 6, 2009
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): May 20, 2024