**University Community (faculty, staff, and students), visitors to the university and independent contractors**

<table>
<thead>
<tr>
<th>SUBJECT (R*)</th>
<th>EFFECTIVE DATE (R*)</th>
<th>POLICY NUMBER (O*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIVERSITY WIRELESS NETWORK INFRASTRUCTURE</td>
<td>April 6, 2009</td>
<td>1910.010</td>
</tr>
</tbody>
</table>

**POLICY STATEMENT (R*)**

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

Rogue or unauthorized wireless access points will be removed from the network to protect the security of FIU’s telecommunications infrastructure.

Florida International University is the sole owner of the unlicensed frequencies on campus.

General access to the network infrastructure, including the wireless infrastructure, will be limited to individuals authorized to use campus and Internet resources. All users of campus and Internet resources must be authenticated. IP address based security or the use of reusable clear text passwords is prohibited. It is expected that applications will require their own general or application specific authentication, authorization and encryption mechanisms to be used by clients entering from any unprotected network.

It is required that wireless devices (e.g., laptop computers) must meet the University’s minimum security standards before access is granted.

Physical security of wireless access points must be maintained to protect the access point from theft or access to the data port.

All wireless communication must meet or exceed the Institute of Electrical and Electronics Engineers (IEEE) 802.11i wireless network security standards.

Wireless devices should not be used for connecting to campus business systems such as human resources, payroll, student information, financial information systems, or other systems that contain sensitive information or are critical to the mission of the University unless a Virtual Private Network (VPN) client is used.

**REASON FOR POLICY (O*)**

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 (R*)

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.

RESPONSIBILITIES (O*)

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):

- 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 be caused 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.
<table>
<thead>
<tr>
<th>RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Division of Information Technology</td>
</tr>
<tr>
<td>Florida International University</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice President and Chief Information Officer</td>
</tr>
<tr>
<td>Florida International University</td>
</tr>
<tr>
<td>11200 S.W. Eighth Street, PC 507</td>
</tr>
<tr>
<td>Miami, Florida 33199</td>
</tr>
<tr>
<td>Telephone Number: (305) 348-2738</td>
</tr>
</tbody>
</table>

The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at [http://policies.fiu.edu/](http://policies.fiu.edu/).

For any questions or comments, the “Document Details” view for this policy online provides complete contact information.

<table>
<thead>
<tr>
<th>FORMS/ONLINE PROCESSES (O*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIU IT Security Blocking Procedures</td>
</tr>
<tr>
<td>Link to the above referenced Form(s) available in the &quot;Document Details&quot; Section of the online version of this policy document.</td>
</tr>
</tbody>
</table>

*R = Required  *O = Optional