NEW COLLEGE OF FLORIDA
REGULATIONS MANUAL

CHAPTER 4 - Academic Affairs

4-5014 Wireless Network

Wireless connectivity presents unique challenges in designing, securing, and managing networks. It has the potential to offer ubiquitous connectivity and great ease of mobility, but if deployed in a haphazard manner, loss of connectivity and mobility is assured and, most importantly, the College's network security system may be compromised.

This Regulation covers general wireless network installation guidelines that must be followed to ensure the College's campus-wide wireless offerings are compatible, provide mobility between locations, and prevent unauthorized access. Any exceptions to this Regulation must be approved by the Office of Information Technology (IT).

(1) Definitions

(a) Wireless Router. Wireless routers are used to support a wireless network in a personal residence. They are sometimes called a wireless DSL or cable router. Some familiar brands are Linksys, Netgear, Belkin, and D-Link.

(b) Wireless Access Point. Wireless access points operate differently than routers. Their sole job is to transmit data between the wired and wireless network without altering the data or changing an Internet Protocol (IP) address. They are transparent to the network. Authentication of individual users is possible since each user is completely visible to the network. Each user is assigned an individual IP address and assignment of those IPs are controlled centrally. By centrally controlling what IP a client is assigned, unregistered clients are restricted in what they can access. Central management of the client registrations doesn't require any configuration on the access points.

(2) Wireless routers are not permitted on the College's network. Any wireless router found on the College's network will have its connection turned off immediately. A wireless router placed on the College's network may cause not only the College's networks to fail, but may cause users of that wireless router to lose connectivity to network technology resources and the Internet.

(3) In order to provide a common authentication methodology for use on all the College's open access (wired and wireless) networks, the College will only deploy equipment that supports central authentication.

(4) Notification of Proposed New Wireless Access Point Installations

(a) Any new Wireless Access Point installations contemplated by College departments must be coordinated with IT's network management team.

(b) The network management team will place and configure the access points so that they do not interfere with other access points already deployed. Each new access point will be placed on the same network as all of the other access points on campus. This will allow mobility between access points.

(c) In order to provide a seamless, manageable wireless network, the College will standardize on a single vendor for wireless installations that is compatible with the existing network management infrastructure and allows configuration of security protocols.

Authority: Article IX, Sec. 7, Fla. Constitution; Fla. Board of Governors Regulations 1.001 and 3.0075

History: Adopted 09-08-12; Revised 02-24-17 (technical amendment)