PROCEDURE

SUBJECT	PROCEDURE: INFORMATION TECHNOLOGY WIRELESS COMMUNICATIONS	PAGE P6.9014-1
LEGAL AUTHORITY	P6Hx23-6.9014	4/17/12 Revision #12-4

P6Hx23-6.9014 PROCEDURE: INFORMATION TECHNOLOGY WIRELESS COMMUNICATIONS

I. Purpose

The College provides access to wireless communications via separate wireless networks for administrative, public, and student uses. This policy specifies access criteria for wireless users and the conditions under which wireless devices may operate when connected to St. Petersburg College's networks.

II. Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of St. Petersburg College's networks. This includes any form of wireless communication device capable of transmitting packet data (e.g.: 802.11a-n, WiFi, BlueTooth, etc.). Wireless devices and/or networks without any connectivity to St. Petersburg College's networks do not fall under the purview of this policy.

III. Compliance Requirements

Only wireless devices meeting the standards specified below or those which have been granted an exclusive waiver by the director of Network Systems are approved for connectivity to St. Petersburg College's networks.

A. Students, faculty, staff, visitors, and other members of the general public must be authorized via user ID and password authentication before connecting to St. Petersburg College's wireless networks. Such authorization may be obtained as described in the foregoing sections of this policy.

B. Students, staff and faculty must enter their assigned College user ID and password to log on to SPC wireless networks.

C. Members of the general public are required to use an assigned user ID and password to log on to the wireless network. Proof of identification is required in order to

register for an individual user ID and password. This assigned user ID and password must be used to log on to the wireless network.

D. Special visitors, events or classes may be given specific instructions for access to college wireless networks as approved by the director of Network Systems.

E. All wireless access points and other related wireless equipment must be approved and registered with the College's director of Network Systems or his/her designee prior to purchase or installation on St. Petersburg College's networks.

F. All such devices will be configured and maintained by the College's Network Systems and Network Academic Support staff unless explicitly authorized by the director of Network Systems.

G. All such devices will be configured to authenticate via the centralized authentication system unless an explicit exception is granted by the director of Network Systems.

H. All computer systems accessing the College wireless networks shall comply with the Information Systems Computer Security Policy, Rule 6Hx23-6.9017.

IV. Limitations

A. Because of the "public" nature of the Public Wireless Network, all connections and usage are at the risk of the Public Wireless Network user.

B. The College accepts no responsibility for protecting the privacy of information transmitted via the student and public wireless networks or wireless devices.

PROCEDURE

SUBJECT	PROCEDURE: INFORMATION TECHNOLOGY WIRELESS COMMUNICATIONS	PAGE P6.9014-3
LEGAL AUTHORITY	P6Hx23-6.9014	4/17/12 Revision #12-4

V. Enforcement and Consequences

The College's Network Systems staff will scan the College network periodically for unauthorized wireless devices. Any such devices will be disconnected from the St. Petersburg College Network and/or impounded to a secure location pending an assessment of an incident by the campus provost or vice president of Information Systems.

Violation of this policy may result in the revocation of access to all St. Petersburg College information technology resources.

History: Adopted - 4/17/12. Effective – 4/17/12.