JAMESTOWN COMMUNITY COLLEGE		
SUBJECT: Wireless Network Procedure	**REFERENCE:**	**ADOPTED:** January 2006 **REVISED:** 2/6/12, 5/7/13, 3/21/14, 7/13/15
SUBMITTED BY: Hardware Network Services	**APPROVED BY:** Vice President of Administration–January 2006 **REVIEWED BY:** Information Security Committee – 5/7/13, 3/21/14, 7/13/15	

I. SCOPE:

This policy applies to all wireless network devices and infrastructure utilizing JCC IP space (including private IP space within JCC networks) and all users of such devices, and governs all wireless connections to the campus network backbone, frequency allocation, network assignment, registration in the Domain Name System, and services provided over wireless connections to the campus network backbone to colleges, departments, or divisions of JCC.

II. AUTHORITY:

This procedure is under the authority and oversight of the Vice President of Administration.

III. DEFINITIONS:

A. **Wireless Network** means local area network technology that uses radio frequency spectrum to connect computing devices to college, department, and division wired networks and may connect to the Campus Network Backbone and the Internet.

B. **Access Point** means electronic hardware that serves as a common connection point for devices in a wireless network. An access point acts as a network hub that is used to connect segments of a LAN, using transmit and receive antennas instead of ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and can be connected to the wired network, allowing access to the campus network backbone.

C. **Wireless Infrastructure** means wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

D. **Interference** means the degradation of a wireless communication signal caused by the electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.

E. **Privacy** means the condition that provides for the confidentiality of personal, student, faculty and staff communications, and institutional and patient data transmitted over a wireless network.

IV. PROCEDURE:

A. The wireless network is not meant as a replacement for the wired network and is not to be used as a primary network connection. The wireless network is meant to extend the wired network for simple uses in areas where wired network access is unavailable. There is no implied network security or privacy provided by wireless network connection. The user must be aware that any information

transmitted via the wireless network may potentially be accessed by others. Users are expected to avoid using applications that will use large amounts of bandwidth. These include servers and file-sharing applications.

B. There are other electronic devices that use the same 2.4Ghz/5Ghz frequency as the JCC wireless network. These devices include 2.4Ghz/5Ghz cordless phones, microwave ovens, X10 wireless camera, Bluetooth devices, and other wireless LAN equipment. Devices using this technology can cause intermittent failure and loss of service. The technology department may investigate and mitigate possible sources of interference.

C. The following policies are in addition to the JCC Acceptable Use Policy. Actions that are detrimental or inappropriate when accessing the college's resources include but are not limited to those listed in the Wireless Networking section below.

1. Users may not extend or modify the network in any way. These include adding access points and installing bridges, switches, hubs, or repeaters. The college reserves the right to remove and disable any unauthorized access points.

2. Any attempt to break into or gain unauthorized access to any computers or systems from a wireless connection is prohibited.

3. Running any unauthorized data collection programs on the wireless network is prohibited. Such practices are a violation of privacy and constitute the theft of user data.

4. We reserve the right to limit bandwidth on a per connection basis on the wireless network, as necessary, to ensure network reliability and fair sharing of network resources for all wireless users.

5. All computers using the wireless network must have current anti-virus software installed.

6. Any effort to circumvent the security systems designed to prevent unauthorized access to any JCC wireless network may result in suspension of all access and an appearance before the appropriate disciplinary authority.