Title of Procedure: Faculty and Staff Wireless Use Procedure

Procedure (check one)  New__X__ Revised ____

Applies to (check all that apply):
Faculty__X__  Staff__X__  Students____
Division/Department____  College____

Background to Issue/Rationale for Procedure:

This standard operating procedure provides guidelines for the usage of wireless technology for faculty and staff. This procedure prevents inappropriate use of wireless network access that may expose BCCC to multiple risks including viruses, network attacks and various administrative and legal issues. This procedure is an extension of the BCCC's Faculty/Staff Computer Use & Internet Access Policy, No. 3000-1

This procedure is subject to change as new technologies and methods of implementing these technologies emerge.

State/Federal Regulatory Requirements:

The State Information Technology Security Policy and Standards can be found at www.dbm.maryland.gov

Information regarding Internet laws and the illegal use of the Internet for Cybercrimes such as investment fraud, child pornography, identity theft, intellectual property, etc. can be found at:
http://www.cybercrimelaw.org/
http://www.usa.gov/Citizen/Topics/Internet_Fraud.shtml
http://www.cybercrime.gov/reporting.htm
http://www.oag.state.md.us/consumer/link.htm

Procedure Language:

It is the procedure of BCCC to provide wireless access to authorized faculty and staff at BCCC's campuses and off-site locations. Wireless access to network drives and the Internet is another way that CITS provides technology support to promote institutional effectiveness. Faculty and staff now have the capability of accessing information away from their desk and without being confined to buildings and locations with active network ports.
STANDARD OPERATING PROCEDURES

A. Usage

a. Wireless Networking procedures are needed to:
   i. Support the Academic Mission of the College.
   ii. Promote greater security in campus networking.
   iii. Protect all wireless resources owned or managed by BCCC.
   iv. Protect all users and uses of BCCC’s wireless resources.

b. Wireless use applies to computing devices such as workstations and laptops.

c. Wireless access is currently available at some locations; however, effective September 2008 wireless access will be available at both the Liberty and Harbor Campuses, BCED, and Reisterstown Plaza locations.

d. CITS has implemented a high level of security, reliability and privacy when using the wireless network. However, users should refrain from running high bandwidth applications and operations such as downloading large music files and videos from the Internet. Network reliability is determined by the level of user traffic and accessibility.

B. Terms, conditions and rules

i. Only authorized faculty and staff will be granted access to BCCC’s Wireless network. Authorization will be determined by the senior management staff of each division.

ii. Faculty and staff must use computing devices owned by BCCC to access wireless resources.

iii. All BCCC owned computing devices will be configured by CITS.

iv. Not all wireless adaptors or drivers support the recommended requirements and may not work with BCCC’s Wireless Network. Therefore, some older computing devices may not be compatible with the existing wireless infrastructure.

v. The college cannot be held responsible for connection failures, Internet service disruption, hardware failures, non-compliant software or denials of service.

vi. Above and beyond the normal network usage policy, wireless usage will be monitored to gauge bandwidth, system traffic and data transmission levels.

vii. All faculty and staff using BCCC’s Wireless Network are prohibited from using file sharing or "peer-to-peer" software for illegally downloading copyright materials. Some of this software has licensing terms that purport to grant external agencies certain rights to use the individual’s computing storage areas. Many users do not realize that these programs may run 'hidden' in the background and use an individual's Internet access and bandwidth. This could have serious effects on the performance of both BCCC’s network and the computer. Use of such software will be monitored on the network and further action will be taken for illegal transfer of copyright.
material.

viii. Access to printers will not be available.

C. Recommended Hardware and Software

i. A minimum of Windows 2000, XP SP2 (Professional editions.)
ii. The latest Microsoft Security updates.
iii. Up-dated anti-virus and anti-Spyware software
iv. A compatible 802.1 1a/b/g wireless adaptor.