Baltimore City Community College

Changing Lives...Building Communities

Policy No.: 3006

Title of Policy: Faculty and Staff Wireless Use

Policy (check one) **New**__X__ **Revised** _____

Applies to (check all that apply):
Faculty____ Staff____ Students____
Division/Department____ College__X__

Background to Issue/Rationale for Policy:

This policy enforces appropriate use of BCCC's wireless resources, inclusive of network drives and the Internet for faculty and staff. This policy is an expansion of the Faculty and Staff Computer Use and Internet Access Policy, and includes specific information regarding the use of BCCC's Wireless Network and Internet access.

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

Proposed Policy Language:

It is the policy of BCCC to provide wireless access to faculty and staff at BCCC's campuses and off-site locations. Users will have access to network drives upon request and the Internet in order to perform college related business. Please note that network drives have confidential and sensitive information that should not be shared or exposed to unauthorized individuals, regardless of the environment (wireless or wired). Therefore, faculty and staff are warned to safeguard their passwords when logging-on to the any of BCCC's networks – wireless and wired. Under no circumstances should passwords be shared with colleagues, family, and friends. In addition, faculty and staff

are required to log-off their computers when leaving the computing area (any campus location with wireless access) for extended periods of time and setup a password-protected screen saver for short intervals away from their computers. It is absolutely imperative that all users exercise extreme caution when accessing information from BCCC's network drives and other related resources.

Wireless access privileges will only be maintained by BCCC's faculty and staff who are in full compliance with this policy, in order to protect the college from potential risks, including but not limited to, unauthorized computer access, network security breaches, unauthorized and inappropriate use of stakeholders' confidential and personal information, virus attacks, malicious intent, and liabilities.

All faculty and staff have the responsibility to use BCCC's wireless resources in an ethical and lawful manner. BCCC has the right, but not the duty, to monitor any and all aspects of the wireless network infrastructure to ensure compliance with this policy. Any user in violation of this policy would immediately lose their wireless privilege and be subject to disciplinary action, including sanctions leading to termination.

Implementation Date: October 28, 2008

Approved by Board of Trustees: October 28, 2008

Originator/Division: Computer Information Technology Services