



Wireless Communications Policy

1. Purpose

The Brunswick Community College's (hereinafter "College") computing and telecommunication networks, computing equipment and computing resources are owned by the College and are provided to support the academic and administrative functions of the College. Federal and state law, and College policies and procedures govern the use of this equipment and technologies. Any additional requirements must be in compliance with applicable federal and state laws, and this policy.

Wireless communications networks use radio waves as a transport medium in lieu of copper cables to transmit voice and data signals. As such, they permit wireless-equipped communications devices to have mobile access to the College (wired) network wherever wireless communications access points are installed.

The purpose of this policy is to set the standard for network operation and security, specifically in the context of wireless network access. The configuration, installation, and maintenance of wireless communication network access point devices, if unmanaged, could result in severe interference with other network users and serious security risks.

Information Technology Services (ITS) defines the standards for the use of networks, including the wireless communications spectrum on campus.

2. Scope

This policy applies to all faculty, staff, students, and others who use the wireless communications spectrum. Adherence to the policy will help protect the integrity of the campus wireless network and mitigate security risks.

3. Policy

A. The Wireless Spectrum

1. BCC regulates and manages all unlicensed radio frequencies on campus.
2. Wireless equipment installed by ITS uses either the FCC unlicensed 2.4 GHz Industrial/Scientific/Medical (ISM) band or the FCC 5.0 GHz Unlicensed National Information Infrastructure (U-NII) band.
3. Wireless equipment transmissions within the 2.4 GHz and 5.0 GHz bands conform to current IEEE 802.11 wireless LAN specifications.
4. ITS may restrict the use of any potentially interfering wireless radio device in College-owned buildings and all outdoor spaces on the BCC campus.
5. Faculty who believe they have special wireless needs should contact ITS.

B. Wireless Network Operation and Security

1. The enterprise wireless infrastructure is managed campus-wide by ITS as part of the College's telecommunications network through the implementation of CISCO equipment.
2. ITS will provide spectrum tuning, and general device management per access area according to wireless access device management standards.



3. Wireless networks will be segmented and treated as a “foreign/untrusted network” from a security standpoint. A firewall, router/switch VLAN technology, or similar technology will be employed to provide this segmentation.
4. Wireless users must be authenticated with unique user credentials.
5. Wireless traffic involving data classified as *Restricted* under the [Data Classification Policy](#) must be used only during registration periods and under the regulations of ITS.
6. Only authorized access points will be permitted. Unauthorized access points will be disabled.
7. Unauthorized traffic interception and/or bridging between the wired and wireless network is prohibited.
8. Applications supported over the wireless network will be limited, as long as this is necessary to provide an acceptable quality of service for all users.
9. No wireless spectrum interference or disruption of other authorized communications is permitted.

4. Enforcement

ITS will enforce the *Wireless Communications Policy* and establish standards, procedures, and protocols in support of the policy.

ITS has the authority to disconnect network service or modify/enhance network security without notification in the event of law violation, systems compromise involving Restricted data as defined by the [Data Classification Policy](#), or negative network communications impact affecting service for other users.

5. Review

The Director of Information Technology Services has submitted the *Wireless Communications Policy* to the Board of Trustees for approval and will periodically review the policy.

6. Links to related College policies

[Security of Networks and Networked Data Policy](#)
[Acceptable Use of Computing and Electronic Resources Policy](#)
[Data Classification Policy](#)