Brock University

WIRELESS SECURITY POLICY

PURPOSE

The purpose of this Policy is to secure and protect Brock University's electronic information assets from wireless security threats. Brock provides computer devices, networks and other electronic information systems to meet the University's missions and goals. Brock provides wireless network connectivity as a service and must manage wireless infrastructure devices responsibly to maintain the confidentiality, integrity and availability of all information assets.

This Policy specifies the conditions that wireless infrastructure devices must satisfy to connect to Brock's network.

SCOPE

All employees (i.e., faculty, staff), students, contractors, consultants and service providers must adhere to this Policy. In addition, this Policy applies to all affiliated and non-affiliated third parties that use the University's wireless infrastructure.

This Policy applies to all wireless infrastructure devices that connect to a University network or that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, mobile phones, tablets and game consoles. This includes any form of wireless communication device capable of transmitting packet data.

If any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail, unless the Policy provision is required by law, in which case the Policy provision will prevail.

POLICY STATEMENT

Responsibility for electronic communication resources resides with Information Technology Services ("ITS").

All wireless infrastructure devices that reside at Brock University and connect to a University network, or provide access to sensitive University information must:

- Abide by the Standards for Wireless Security
- Use Brock-approved authentication protocols and infrastructure
- Use Brock-approved encryption protocols
- Maintain a hardware address (MAC address) that can be registered and tracked.

COMPLIANCE AND REPORTING

ITS enforces this Policy and the related Standards at all times. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to promptly report it to the ITS Help Desk. Policy violations that come to the attention of the ITS Help Desk will be escalated to the IT Security Specialist.

Policy violations will be assessed, and action taken to remediate the violation subject to collective agreements and / or other contractual conditions.

Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be escalated to the Associate Vice-President ("AVP"), ITS for further action. Periodically, the AVP, ITS will provide to SAC a summary of all policy violations.

Policy owner:	Associate Vice-President, Information Technology Services
Authorized by:	Current version: Executive Team Prior versions: Board of Trustees, Capital Infrastructure Committee
Accepted by:	SAC
Effective date:	December 2021
Next review:	December 2022
Revision history:	2020 2019 2017 2016
Related documents:	Standards for Wireless Security