STANDARDS FOR WIRELESS SECURITY

PURPOSE

A standard includes specific low level mandatory controls that help enforce and support a policy.

The purpose of this document is to support and outline in detail the requirements of the Wireless Security Policy. These requirements are mandatory and must be adhered for all wireless connectivity and deployments.

Wireless deployments

- ITS will install, configure and maintain all wireless access points that connect to the University's campus network. Prior to installation, ITS will complete a site survey that will be used to determine optimal access point locations and types
- Wireless access points must be connected to network switches directly and not use network hubs.

Wireless infrastructure

Wireless network identifiers

Network Identifier - SSID	Typical User	Characteristics
BrockWifi	Staff, Faculty, Students	• Authenticated • Encrypted
eduroam	Eduroam users, Staff, Faculty, Students	• Authenticated • Encrypted
BrockEvents	Conference users	• Used throughout the year to facilitate Conference Services or during major special events • Unencrypted
ResIoT	Residence Students with non WPA2-Enterprise capable devices	• Unencrypted • Authenticated via MAC address

Wireless encryption and authentication

- Encrypted wireless networks at Brock must use WPA2-Enterprise encryption
- Encrypted wireless networks must use 802.1X standard for authentication.

Wireless frequency

- The 2.4GHz and 5GHz radio frequencies are unlicensed and shared, and therefore are susceptible to interference
- Access points can interfere with each other as well as with appliances such as microwave ovens and cordless phones
- ITS will manage the shared use of unlicensed radio frequencies for the campus community and has the authority to resolve interference issues
- The appropriate action to resolve such interference may include tuning or removal of devices which are causing the interference.

Any exception to the requirements in this Standard must be documented and approved by the Director, Infrastructure.

Wireless network definitions

IEEE 802.11: A set of standards from the Institute of Electrical and Electronics Engineers Standard Association (IEEE) for implementing wireless local area network communications.

Service Set Identifier (SSID): A term in the IEEE 802.11 standard describing a unique identifier for a wireless network.

WiFi: WiFi is a broad term describing technology that allows an electronic device to connect and exchange data using 2.4GHZ or 5GHZ radio waves.

Wireless Access Point (WAP): A device that allows wireless devices to connect to a wired network.

WPA2-Enterprise: WiFi Protected Access 2 Enterprise provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1x-based authentication. Also referred to as WPA2-802.1X mode, this is designed for enterprise networks and requires a RADIUS authentication server.

802.1X: IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.