POLICY 1.21 – Wireless Networking Policy

Policy Category: General
Effective Date: April 28, 2005
Revised: (NEW)

PURPOSE

1.0 The purpose of this policy is to increase the reliability and security of the wireless network access at The University of Western Ontario. Wireless networking uses limited shared unlicensed radio spectrum across campus. Careful planning, management and cooperation are required to support the implementation and use of wireless access across campus. Wireless networks are considered an augmentation of the University wired network which the University owns and manages through Information Technology Services (ITS).

2.0 A wireless networking policy is needed:

- To support the academic mission of the University
- To limit interference with the University’s current and future network infrastructure
- To promote greater IT security on campus

SCOPE

3.00 This policy applies to all wireless networks and users of wireless networks at The University of Western Ontario that connect to or affect the Western campus backbone network.

POLICY

4.00 Management of radio spectrum on campus

- ITS is responsible for managing wireless networking services on campus. Other departments may deploy wireless network access points or other wireless service on campus in coordination with ITS. Private wireless access points in residences or offices are required to comply with the UWO standard.
- ITS is responsible for the management of wireless spectrum usage at UWO. ITS may restrict use of any devices that can cause interference in the unlicensed radio spectrum used for wireless networking at UWO.
- ITS is authorized to scan for rogue access points and to block access to the UWO backbone network to those that are detected.
- ITS is responsible for maintaining a secure network and will deploy adequate security procedures to support wireless networking on campus.
- Encryption of wireless communications is required for all Staff and Faculty at the University of Western Ontario, and recommended for students.
- Any issues arising from research involving wireless networking will be resolved in cooperation with ITS, the researcher in question and/or the Vice-President (Research & International Relations).
REQUIRED SECURITY

5.00 The wireless LAN implementation at the UWO must be done in accordance with a security plan. This plan must address the following issues:

(a) Restricting network access so only authorized users can connect.
(b) Preventing unauthorized users from viewing confidential data appearing on the wireless infrastructure, particularly passwords.

To the extent possible, all wireless users must use auto-update antivirus software and ensure that their machines are fully patched.