POLICY TITLE:	**Wireless Local Area Network Policy**
POLICY #:	**CIO-ITSecurity-07.4.2**
Initial Draft By - Position / Date:	Jim Lennie, Manager, Networking Services, April 2004
Approved By / Date:	**ISC – May 5, 2004**
Last Revised Date:	**April, 2010 Reformatted to CIO Policy Template and content substantially updated.**
Next Review Date:	Two years after approval.
Brief Description:	**This policy applies to all uses of WLAN technologies at all physical locations on the University campuses, both inside buildings and outdoor areas.**

Purpose

- Guide the deployment of wireless local area networking (WLAN) on the University of Guelph campuses to ensure reliable, compatible, and secure operation.
- Protect the security of the University's information resources and electronic communications.
- Arbitrate possible interference of other wireless devices with the University wireless network.

Scope

This policy applies to all uses of WLAN technologies at all physical locations on the University campuses, both inside buildings and outdoor areas. Exceptions may only be granted by the Chief Information Officer (CIO). It does not apply to cellular wireless technology.

All University of Guelph policies and procedures apply to the use of the WLAN's.

Background

The university network infrastructure is a centrally managed, shared resource. As such, expansion or modification of the infrastructure must be undertaken with consideration for capacity, availability and security. Computing and Communications Services (CCS) is mandated to develop and maintain the university's networking infrastructure.

The University WLAN is an established, critical component of this infrastructure which supports teaching, learning and administration. It offers an opportunity for faculty, staff, and students to take advantage of access to university network facilities from areas outside of traditional hard-wired network locations. Examples include lecture halls, large open areas like food courts, outdoor areas and green houses. This policy addresses the use of the radio airspace used by wireless technology and the operation of WLAN devices and systems.

Policy

In order to provide the best possible quality of wireless network service, ensure wired and wireless network security and integrity, the University WLAN will be a centrally managed service and governed by the following set of policies.

1. CCS will have sole responsibility for design, specification, installation, operation, maintenance, and management services for all access points. Any University college or directorate seeking to establish or expand existing WLAN capability will contract with CCS for the installation.
2. Individuals and departments must not independently deploy access points. CCS will work with any University department wishing to establish or expand WLAN networking in their area.
3. The use of the University WLAN shall be subject to the University's Acceptable Use Policy and Guidelines for computing and networking facilities.
4. The University WLAN operates in the unlicensed 2.4 GHz and 5GHz range. Other wireless devices use the same frequency bands and may disrupt the operation of the University WLAN. If interference occurs, the University WLAN will have priority. In cases of significant problems, users of other devices will be required to cease using those devices.
5. All access to the wireless network must be authorized through the use of either a) University of Guelph central login account and password or b) credentials provisioned by authorized administrators for the explicit purpose of connecting to the University's network resources.
6. Where applicable, devices accessing the University WLAN must have up to date anti-virus software and operating system updates installed.

Implementation of Policy

The implementation and enforcement of the University WLAN policy will be guided by the following considerations.

1. CCS will monitor the University WLAN to detect independently installed access points or other wireless devices that could potentially impact on the security and/or availability of the wireless network. Owners or administrators of these access points will be requested by email to disconnect their non-conforming devices. In the event of suspected interference or other adverse impact on the University WLAN or users of the University WLAN, or in the event that a non-conforming device persists following two (2) electronic warnings, CCS is authorized to disconnect or suppress the signal of the non-conforming device. Under these circumstances CCS will formally notify the Departmental Chair/Manager of the action which has taken place.
2. Devices connecting to the University WLAN will undergo an assessment of installed anti-virus software and applied system patches. WLAN access may be restricted or prevented until anti-virus software has been installed and/or updated, and system software patches provided by the operating system vendor have been installed.
3. In cases where interference occurs between a wireless device used for a specific teaching or research application and the WLAN, CCS will work with faculty to mitigate the interference and try to accommodate the device without disrupting the teaching or research activity, or the University's WLAN.
4. All exceptions to point #2 above must be documented in a formal Service Level Agreement (SLA) between CCS and the applicable unit which is subject to review and approval by the Chief Information Officer (CIO) or designate.
5. The Chief Information Officer (CIO) is responsible for the enforcement of the University WLAN policy.

Definitions

Access Point: a wireless communications hardware device that creates a central point of wireless connectivity. A wireless access point behaves much like a "hub" in that the total bandwidth is shared among all users for which the device is maintaining an active network connection.

Coverage Area: The geographical area in which an acceptable level of wireless connection service quality is attainable. Coverage areas for similar devices can vary significantly due to the presence of building materials, interference, obstructions, and access point placement.

Interference: Degradation of a wireless communication radio signal caused by electromagnetic radiation from another source including other access points, cellular telephones, microwave ovens, medical and research equipment, and other devices that generate radio signals. Interference can either degrade a wireless transmission or completely eliminate it entirely depending on the strength of the signal generated by the offending device.

WLAN: "Wireless Local Area Network". The term often used for a wireless network within a limited area consisting of one or more access points that provide network connectivity to computers equipped with wireless capability (usually a notebook computer with a wireless PC card). In essence, a WLAN provides the functionality of a wired LAN without the physical constraints of the wire.