UCIT Data Network Standards

Campus Wireless Network Standard

Classification IT Infrastructure	Table of Contents by Section
Standard # IFS-001	
Approval Authority Chief Information Officer	
Implementation Authority Director IT Infrastructure	
Effective Date	
Latest Revision June 18, 2009	

Rationale **1**

1.1. Standardization of the U of C's 802.11 wireless networks and frequency bands is required to insure availability of the wireless network to the campus community. Standards of use will improve the wireless service and help to ensure appropriate security and reduced operating and support costs.

1.2. UCIT Network Services has the mandate to manage the wired and wireless networks on campus and manages the wireless air space at the University of Calgary.

1.3. Other Access Points (AP) and devices that produce frequencies in these ranges may interfere with the operation of the campus WLANs. Wireless networks can reach beyond intended spaces and unauthorized users may attempt to connect to access points that, in turn, give them access to U of C networks and resources.

Scope **2** This standard applies to all uses of WLAN technologies at all physical locations on the University of Calgary campuses, both inside buildings and outdoor areas. This standard does not apply to cellular wireless technology.

Definitions **3** Access Point (AP)

A wireless communications hardware device that creates a central point of wireless connectivity using Wi-Fi.

Coverage Area

The physical and geographical area in which an acceptable level of wireless connectivity can be attained. Signal strength in these areas may vary significantly due to factors such as distance from the access point, radio interference, building materials, and other physical obstructions.

Interference

The degradation of wireless radio signals caused by electromagnetic radiation from sources such as other access points, cellular phones, microwave ovens, medical and research equipment, and other devices that generate radio signals.

Network Owner

All networks at the University have an official owner, which may be a faculty, department, research group, or other university-affiliated organization. These owners have full control over who may have access to their network wherein permission must be sought in order to attach wireless access points to it.

Rogue Access Point

Any access point on campus installed without the permission of the network owner or IT Network Services.

Secure Network

A secure campus network that is allowed to access Administrative services and mainframe data and that is under the direct control of a UofC staff member.

SSID

Service Set IDentifier is the public name of a wireless network.

WLAN

Acronym for "Wireless Local Area Network". The term is often used for a wireless network within a limited area that consists of one or more access points which provides network connectivity to computers and devices with wireless capability.

Standards **4** 4.1. U of C wireless networks operate in the following unlicensed frequency bands:

- 2.400-2.483 GHz
- 5.15-5.35 GHz
- 5.470-5.725 GHz
- 5.725-5.825 GHz

4.2. The campus wireless network will be integrated into the Data Network Standard in buildings as the infrastructure is upgraded. All new AP deployments will be connected to 1 Gbps POE switches which will then be connected to the building head end switches.

4.3. Wireless Standard WiFi alliance Pre-Standard certified 802.11n compliant access points shall be deployed for all new buildings and major retrofits. These APs must be able to integrate with the U of C's wireless management system.

4.4. All wireless access point deployments must be approved by the CIO. UCIT Network Services will assist any individual or group wishing to install a wireless network in their area.

4.5. Written Permission must be obtained from the owner of the network and the CIO prior to the deployment of any AP. Rogue APs (those without proper authorization) will be subject to removal.

4.6. APs must not be deployed on an Admin or Secure Managed Client network. If a rogue AP is discovered on a secure network, the network will be decertified until the rouge access point is removed.

4.7. AP SSIDs must be registered with UCIT Network Services by summiting completed Wireless Network SSID Registration Forms (http://www.ucalgary.ca/it/networks/wireless/standard/form).

4.8. An authentication scheme must be employed so that non-authorized users (those without a valid UofC account) cannot access authorized APs.

4.9. Electronic devices operating in the frequency bands listed in 4.1 may interfere with the campus wireless network. These devices may include wireless APs, faulty microwave ovens, or certain wireless telephones. UCIT Network Services will work with users and departments to eliminate interference with the campus wireless network. UCIT Network Services reserves the right to disable or remove any AP or other electronic device that is disrupting the operation of the campus WLAN or other registered wireless LANs.

Exceptions **5** The CIO can approve exceptions to the above standard. Exception requests must include detailed descriptions of:

a. Why the proposed solution is being requested rather than following the standard.
b. How the proposed solution varies from the standard?
c. What are the implications for long term management of the variation

Parent Policy **6**

Related Policies & Standards	**7**	Acceptable Use of Information Assets Policy Information Asset Security Monitoring Policy Information Asset Protection Policy Data Network Standard		
History	**8**	Oct 15, 2008	Tom Rolff, Jim Powlesland	Initial draft
		Oct 22, 2008	Doug Doran	Revise format
		May 7, 2009	Doug Doran	Revise format and content
		May 8, 2009	Dennis Tracz	Revise format and content
		June 6, 2009	Doug Doran	Revised wording
		July 9, 2009	Doug Doran	Updates and format changes