



UU Security Policy

Wireless Communications Policy

Author:	Harry Young
Approved by:	IICTSC
Version:	2.0
Date:	1 June 2006
Status:	Agreed
Classification:	Public
Enquiry point	Harry Young Network Manager University of Ulster Phone: 028 90366488 Email: h.young@ulster.ac.uk
Policy effective from:	1 Sept 2004
Policy review date:	1 May 2007

Change History

Version	Changes	Date
1.0	Initial document	1/9/04
2.0	Included BS7799 reference Change department name to CIS	1/6/06

Contents

UU Security Policy	1
Wireless Communications Policy	1
Change History	2
Contents	2
Wireless Communications Policy	3
Reason for Policy	3
Corporate Information Systems (CIS) Service Provision	3
Departmental Wireless Networks	3
Security	4
User Requirements	4
Enforcement	5
Further Information	5
BS7799 Reference	5

Wireless Communications Policy

Reason for Policy

This policy describes how wireless technologies are to be deployed, administered and supported at the University of Ulster. The implementation of this policy assures that all constituents using wireless communication networks receive an acceptable baseline level of service quality with respect to reliability, integrity, availability and security.

Corporate Information Systems (CIS) Service Provision

- CIS shall deploy all University Wireless Access Points.
- To protect the integrity of the University network infrastructure and prevent unauthorised access, all open wireless access areas will be connected to a separate wireless VLAN through a gateway service which will be used to permit or deny access to the University network.
- To be granted access to the University network wireless clients will have to authenticate at the wireless gateway. Authentication and authorisation will be based on University approved user accounts.
- Following authentication a limited range of supported applications will be permitted.
- CIS encourages the connection of all wireless access points to the University wireless VLAN.
- CIS will manage and monitor the usage of the open wireless network as it does the wired network.
- CIS will monitor the development of the wireless network technology, evaluating wireless network technology enhancements and as appropriate incorporate new wireless network technology within the University network infrastructure to meet business and security requirements.

Departmental Wireless Networks

- Departments who wish to install wireless access points should in the first instance discuss their requirements with a member of the CIS network team. Wireless access points must be registered with CIS and use only the wireless channels and IP addresses allocated by CIS.
- Where a department installs a private wireless access point to support its teaching and research purposes, security on such a network is the responsibility of the department concerned. At a minimum it should:
 - Authenticate all user access, ensuring that only known staff members have access. The system must only allow known specified MAC addresses to join the network.
 - Be able to identify users in cases of reported misuse.

- Encrypt communications between clients and the wireless access point.
 - Change the SSID (service set ID) from the default and if necessary disable its broadcast.
 - Change the default wireless channel.
 - Ensure the access point is connected to a dedicated Ethernet switch port.
- Where a departmental wireless access point interferes with a central service provision or prevents campus wireless provision in that area, then the departmental network must defer to the centrally provided service if a workable solution is not available.

Security

Wireless networks are inherently less secure than wired networks. Because the signal is broadcast the wireless network is shared and any wireless device can listen to network traffic from any other wireless device that is in range. Without using any application to support security and privacy, the wireless network must be regarded as being open and not secure.

- Unless using encrypted protocols on secure Wireless Access Points, wireless clients must not be used for connecting to UU business systems such as human resources, payroll, student information, financial information, or other systems that transmit sensitive or confidential information or that are critical to the mission of the University.
- Staff must not use wireless access in student areas for accessing or transmitting sensitive or confidential information. Access to sensitive or confidential information should only be from secure wired network connections.

User Requirements

- Under no circumstances is any student permitted to connect any form of Wireless Access Point to the University Network.
- Users should note that they are responsible for:
- Ensuring their Laptop has up-to-date patches, anti-virus software, personal firewall and other measures to protect it whilst operating on an insecure network;
 - Any equipment that is connected to their system, for ensuring that it is in good working condition and that it will not present a health and safety risk to them, others or University property;
 - Ensuring their Laptop is virus free.
- Users should be aware that:
- Use of a wireless LAN connection in “ad hoc” mode is unacceptable, as it may interfere with legitimate wireless networks elsewhere on campus. Laptops discovered not in infrastructure mode may be

disconnected from the network and/or users will have their user account disabled;

- If found to be using a wireless LAN connection that is consuming high bandwidth, which contributes to a deterioration of the wireless network, it may be disconnected from the network and/or have their user account disabled;
- That the wireless network is not secure;
- Use of the University wireless network implies that they are in agreement with the University Acceptable Use Policy;
- The University will not accept responsibility or liability for any damage to or loss of data to their machine while in transit or connected to the University network;
- Laptops can only be used in designated Open Access Areas;
- That activity on the University network will be monitored and recorded to secure effective operation, and for other lawful purposes.

Enforcement

- Connection of an unauthorised Wireless Access Point to the University network is prohibited. Efficient operation of wireless networks depends on a planned approach to the allocation of the limited spectrum available. Rogue Wireless Access Points (any Wireless Access Point not registered with CIS) jeopardises the integrity of the wireless infrastructure and may interfere with and degrade the performance of authorised services. Surveying and monitoring will be undertaken to locate Rogue Wireless Access Points and any found will be disconnected from the network.
- In the event of any abuse of facilities, CIS reserves the right to withdraw access until the matter has been dealt with by the appropriate authority.

Further Information

Policy on Acceptable Use of University Computing and Data

BS7799 Reference

A 3.1.2	Review and evaluation
A 4.1.3	Allocation of information security responsibilities
A 8.3.1	Controls against malicious software
A 8.5.1	Network controls
A 9.4.1	Policy on use of network services
A 9.4.6	Segregation in networks
A 9.4.7	Network connection control
A 9.7.1	Event logging
A 9.7.2	Monitoring system use

Ref: UU Security Policy / Wireless Communications Policy

Version: 2.0 Status: Agreed

Classification: Public

Page 5 of 5