

(Standard) ICT Standard for Wireless Communications

Document Purpose

Document Purpose	This standard defines the controls that will apply to wireless data networks installed and operated at the University of Southern Queensland to ensure that they will satisfy the service quality, performance and security objectives required to support existing and planned future services provided by the Division of ICT Services.			
Document Information	Version	1.0		
	Release Date	November 2009		
	Release Status	Draft		
	Review Date	November 2010		
	Author(s)	Manager – Data Communications		
	Owner	Chief Technology Officer		
	Print Date	Last Printed:		
	Approved By	Executive Management Team		
	Policy	USQ Policy for ICT Information Management and Security		
	Type of Document	Standard		
	Electronic Location and Filename			
Version Control	Version	Date	Author(s)	Summary of Changes
	0.1	2009	M. Thompson	Document creation
	0.2		T Downs	Amendments
Error Advisory	<p>To the Reader:</p> <p>If you encounter any inaccuracies or printing faults in this document please contact the Owner (see Document Information section, above) as soon as possible. The Owner will then initiate the required modifications</p> <p>If you are unable to contact the Owner, contact that person's Manager Supervisor.</p> <p>Thank you for helping the Division of ICT Services maintain quality documentation.</p>			

Table of Contents

Document Purpose	1
Document Information	1
Error Advisory	1
1 Definitions.....	3
2 Introduction	3
3 Standards.....	4
3.1 Scope	4
3.2 Standards, Services and System Deployment.....	5
3.3 Wireless Security and Authentication	6
4 Related Documents.....	7

1 Definitions

The [ICT Glossary and Definitions](#) contains a description of any common ICT terminology referred to in the policy and standard documentation.

2 Introduction

The Division of ICT Services (DICTS) has implemented and supports Wireless Local Area Network (WLAN) systems on all major campuses. WLAN's will allow campus users to access computing facilities and information sources from portable and mobile computers including hand held devices. WLAN's complement the Universities wired network and deliver benefits including convenience, flexibility, access, deployment and cost.

Wireless communication transmits University information over radio waves which are pervasive throughout the area in which the signal can be received, increasing the opportunity for security breaches and interference with other services. Uncontrolled wireless network access poses significant risks to the security, reliability, and integrity of University information and services, as well as exposing the University to liability risks. University owned or operated networks and devices, and wireless devices connected to the University network or infrastructure services must also be carefully managed to ensure the security, integrity, and reliability of University information and services. Registration and regulation of wireless network users, and regulation of access between wireless networks and public networks such as the internet, are also necessary due to the University's potential obligations as a Carriage Service Provider under the Telecommunications Act 1997 (Cth).

The open nature of wireless networks and transmissions leave them exposed to a number of security threats that must be mitigated through the implementation of specific security requirements and controls.

3 Standards

3.1 Scope

This standard applies to all University of Southern Queensland staff, students, third parties (affiliates and pseudo), visitors, contractors, consultants and any other persons utilising wireless devices to access the University of Southern Queensland ICT resources. It also applies to facilities throughout USQ including University affiliated organizations and to tenancies in University-owned properties.

The Division of ICT Services is responsible for the ICT Wireless Communications implementation, operations and procedures. This standard covers the following:

- The security of the University of Southern Queensland ICT Network;
- Access to University networks via unsecured wireless communication mechanisms is prohibited. Only wireless systems that meet the criteria of this standard, or have been granted an exclusive waiver by the Chief Technology Officer, are approved for connectivity to USQ networks;
- All areas of wireless connectivity to the University network infrastructure are included. This includes all wireless devices operating within the University's IP address range, or any University premises, or any remote location connected to University networks;
- All areas of wireless connectivity to the University network infrastructure, and includes all wireless devices operating within the University's IP address range, or any University premises, or any remote location connected to University networks.
- All wireless data communications devices (e.g. personal computers, cellular phones, PDA's etc.) connected to any University network. This includes any form of wireless communication device capable of transmitting packet data.
- VPN access via the USQ wireless network;
- The use of unauthorised wireless equipment which may be considered a security threat to the University of Southern Queensland and/or authorised clients of the wireless network.

Wireless devices and/or networks without any connectivity to USQ networks do not fall under this standard.

Clients connecting to USQ networks should ensure they read, understand, and comply with all aspects of the following:

- [ICT Standard for Operational Security Management](#)
- [ICT Standard for Networks](#)
- [ICT Standard for the Use of ICT Resources](#)

3.2 Standards, Services and System Deployment

- a) The Division of ICT Services shall be solely responsible for the management and operation of wireless network infrastructure in the USQ network. In the case of WLANs, the line of demarcation is the air interface at the client (i.e. where the user's antenna meets the air). DICTS's responsibility includes all nodes in point-to-point or point-to-multipoint wireless links.
- b) The Division of ICT Services will develop a set of standards to which WLANs and other wireless networks at USQ must conform. (Note: Departments engaged in research networks must ensure that specific equipment and software purchased for research purposes will not adversely affect the production network).
- c) The Division of ICT Services will progressively deploy WLAN services to cover public (including outdoor) areas at USQ campuses.
- d) The Division of ICT Services will deploy and manage WLAN systems to cover most academic areas, including common teaching rooms.
- e) Departments shall not deploy their own production wireless systems because of the security, consistency and interference problems that that would entail. (Note: This does not apply to very low power wireless systems (max 1 mWatt EIRP) designed for short range "personal area networks" e.g. Bluetooth. There is no restriction on the deployment of such systems as long as they are not causing interference with the production network.)
- f) The WLAN service operated by the Division of ICT Services will provide the greatest possible degree of mobility and uniformity to users, consistent with security requirements and technical limitations.
- g) All client wireless devices must conform to appropriate Australian Communications Authority (ACA) regulations (<http://www.dcita.gov.au>)
- h) All client wireless devices accessing the USQ WLAN must be Wi-Fi Certified™ (<http://www.wi-fi.org>)
- i) All client wireless devices accessing the USQ WLAN must support one or more of the following IEEE standards:
 - 802.11a
 - 802.11b
 - 802.11g
 - Note: There is a preference for client devices to support at least two standards (preferably 802.11b and 802.11g)
- j) Client wireless devices should be capable of connecting to USQ WLAN using one of the secure access methods. Information relating to these can be located on the USQ ICT web page (<http://www.usq.edu.au/ict>)
- k) The Division of ICT Services will provide documentation on the methodology of connecting to USQ WLAN for, at a minimum, the operating systems that USQ supports.
- l) Authentication must be encrypted in accordance with encryption standards deemed acceptable by the Division of ICT Services.
 - All encrypted methods must be approved by DICTS. These methods are outlined in the restricted section of the USQ ICT web page.
 - All data transmissions must be encrypted between the client's device and the USQ WLAN
- m) The Division of ICT Services will manage and support all authorised enterprise WLAN access points. Application for exemption for the operation of non-enterprise access points must be made initially to the ICT Manager - Data Communications.
- n) Any wireless device causing service degradation to the USQ network will be shut down.

- o) Non-authorised wireless access points will be considered in breach of the *USQ ICT Policy for Information Management and Security* and disciplinary action provisions will arise.
- p) Risk assessment will be conducted at intervals not exceeding 12 months.
- q) USQ campuses may have their radio frequency spectrum scanned at least once a year at the discretion of DICTS. This will be conducted under the auspices of the Division of ICT Services.

3.3 Wireless Security and Authentication

- a) All WLANs will require each client to authenticate to the network before network access is granted at the start of each session.
- b) The use of the WLAN is restricted to users with a valid USQ userid and visitors with a valid userid from a University participating in the eduroam program. USQ participates in [AARNet eduroam](#). This userid will be the sole method of authenticating to the WLAN.
- c) The Division of ICT Services will determine minimum security measures to be used on WLANs and other wireless data transmission systems. The standard required may vary from one class of user to another, and will change over time depending on available technology, and the degree of risks and threats.
- d) Use and access to the WLAN is governed by the USQ acceptable usage policies and standards.

4 Related Documents

Document (Electronic)	ICT Standard for Operational Security Management available at http://www.usq.edu.au/resources/ict_standard_for_operational_security_management.pdf
Document (Electronic)	ICT Standard for Networks available at http://www.usq.edu.au/resources/ict_standard_for_networks.pdf
Document (Electronic)	ICT Standard for the Use of ICT Resources available at http://www.usq.edu.au/resources/ict_standard_for_the_use_of_ict_resources.pdf