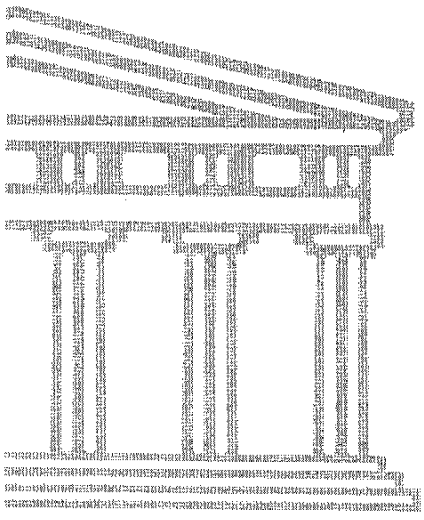

UNIVERSITY OF WESTERN CAPE (UWC)

POLICY FOR
DEPLOYMENT AND MANAGEMENT OF 802.11
AND
RELATED WIRELESS STANDARDS
(WIRELESS POLICY)

DATE OF LAST APPROVAL: C2004/5

UNIVERSITY of the
WESTERN CAPE

A place of quality, a place to grow, from hope to action through knowledge

Policy for Deployment and Management of 802.11 and Related Wireless Standards (Wireless Policy)

University of the Western Cape Policy *ICS/2004.01*

Background

This policy provides the structure for a campus-wide solution for the implementation of wireless technology, which includes centralized determination of identity and authentication to ensure the provision of the appropriate levels of security.

Wireless in the Local Area Network using the IEEE 802.11 standard is a fast emerging technology. 802.11 wireless technologies are by nature easy to deploy, but highly sensitive to overlapping frequencies. Because of these characteristics, all wireless use must be planned, deployed, and managed in a very careful and centralized fashion to ensure basic functionality, maximum bandwidth, and a secure network.

Current 802.11 wireless technologies deploy a very low power signal in a frequency band divided into only 3 non-overlapping channels. The primary purpose of these channels is not so much to provide separate networks, but to ensure that adjacent access points with slightly overlapping areas of coverage do not interfere with each other. In the normal case, it is necessary to use all three channels in an integrated fashion as a single unified network in order to achieve an optimal design. It is therefore not feasible to allow individuals to install their own access points without centralized coordination, due to the resulting signal interference and greatly degraded performance to the common wireless network.

To ensure the technical coordination required to provide the best possible wireless network for the University of the Western Cape (UWC), the campus' Information and Communication Services (JCS) will be solely responsible for the deployment and management of 802.11 and related wireless standards access points on the campus. Other departments may deploy 802.11 or related wireless standards access points, but only provided that such deployment is done in coordination with JCS.

Scope

The Wireless Policy provides guidelines regarding the following:

- the central deployment of wireless access points by ICS based on 802.11 and related wireless standards;
- the provision of wireless service by !CS for campus departments;
- the management by JCS of 802.11 and related wireless access points on the UWC campus.

Policy

I. JCS deployment of wireless access points based on 802.11 and related standards

The University of the Western Cape's Information & Communication Services (ICS) will be solely responsible for the deployment and management of 802.11 and related wireless standards access points on the campus. No other departments may deploy 802.11 or related wireless standards wireless access points without coordination with JCS.

2. Provision of wireless service by ICS

JCS will offer a standard wireless deployment plan that will meet the needs of most UWC departments wishing to construct and operate departmental wireless services. Departments requiring a different wireless deployment plan may contract with res to have res construct and operate either a standard or, if the spectrum is available for it, premium wireless services. res will work with departments to accommodate any special needs they may have within the technical constraints of the wireless technology, understanding that all requests may not be technically feasible. res will provide wireless access points only when it is the most cost effective response to a given scenario and only if it falls within the scope of res responsibility as determined by the Executive Director.

3. Management by res of 802.11 and related wireless standards access points

res will ensure that all wireless services deployed on campus will adhere to campus-wide standards for access control. res will manage the wireless spectrum in a manner that ensures the greatest interoperability and roaming ability for all departments wishing to use wireless technology, and will centralize the process of determining identity, authentication, and appropriate levels of security for access to and use of wireless technology. ICS reserves the right to minimize interference to the common wireless network, and will work with departments to reconfigure or shut down any departmental wireless networks that interfere with the common wireless network.

Procedures and Guidelines

res will advise ou wireless plans, deployment strategies, and management issues.

Any department wishing to work with res to deploy wireless access must contact res by phoning 2000 or e-mailing: helpdesk@uwc.ac.za to begin the process. Departments must also ensure that hardware and software purchased adhere to campus standards.

Departmental wireless networks will be treated as alliance networks as defined in the Network Security Policy; this requires a formal agreement between res and the department.

In the case of existing wireless technology deployments that use the same or interfering spectrums, res will work with the departments in question to minimize interference to the common wireless network.

All sensitive data being transmitted across a wireless network should be encrypted

Responsible Organization

The Office of the Executive Director for Information and Communication Services will be responsible for this policy and for any appeals of res decisions relating to wireless deployments. This policy will be reviewed yearly by ICS, and changes will be authorized by the approval of the Information Systems Committee (CISC). ICS will review LAN wireless access standards on an annual basis and recommend changes to this policy as needed.

Approved by Council on 4 December 2004 (C2004/5)