UNIVERSITY OF PRETORIA

Information Technology Services

Wireless Network Standards and Procedures

Document type: Standard
Policy Category: Professional Service

Document number: ITS1476

Table of contents

1 Introduction

Internet connectivity has become a necessity for both students and staff at the University of Pretoria (“the University”, “the institution”, UP) in the execution of their academic, research and administrative activities. Together with the increased availability and usage of wireless devices the need for wireless network connectivity has grown and will continue to grow.

In order to ensure a fair and sufficient distribution of wireless access points over all University campuses, according to the needs of its potential users, while protecting the assets of the University, such as the radio frequency airspace, the available bandwidth, and the electronic systems and information of the University, the wireless network needs to be protected and governed by relevant standards.

This document covers the principles that will be adhered to in growing the wireless network, standards required to minimise interference in the wireless network airspace, and regulations to provide secured access to institutional assets.

This document prohibits access to the institution’s data network via unsecured mechanisms, and in particular via unauthorised and unsecured wireless network devices. It stipulates standards, conditions, procedures and

guidance to staff, students and guests who wish to have access to the wireless network, or use wireless client devices on institution property.

The document is one of a set of documents informed by the *Information Technology Security Policy* [1] and the *Electronic Communications Policy of the University of Pretoria* [2], which in turn support the *Policy on Acceptable Use of Computing Resources* [3].

2 Organisational scope

This document applies to all wireless data communication devices capable of transmitting packet data (e.g. access points, bridges, personal computers (PCs), laptops, cell phones, tablets etc.) connected to any of the institution's networks on any of the institution's campuses or offices, and operating in 2.4 GHz or 5 GHz bands, and to all persons who connect to the UP wireless network using such devices.

Devices operating outside the 2.4 GHz and 5 GHz bands are generally excluded.[1]

3 Purpose statement

ITS strives to provide wireless coverage in accordance to institutional needs, while managing the wireless service in a secure way that will protect institutional assets from threats to their confidentiality, integrity, and availability.

This document regulates the provisioning and use of the wireless network and addresses, namely:

- Criteria which influence decisions related to the provisioning of wireless access;
- Procedure to request self-funded expansion of the wireless network;
- Regulations to protect the wireless airspace;
- Regulations on managing access to and usage of the wireless network;
- Requirements for client devices used to access the wireless network;
- Support provided by ITS; and
- Responsibilities of ITS and users of the wireless network respectively.

4 Consequences of Non-compliance

Failure or refusal to adhere to the rules detailed in this process shall be deemed as misconduct and line managers may initiate appropriate investigation and disciplinary action against offenders. A claim of lack of knowledge as to the existence and/or application of this process shall not be grounds for justification of non-compliance.

Line managers must ensure that appropriate training and orientation is provided to ensure that the process is implemented and the implementation is maintained.

5 Definitions

Table 1: Technical definitions

Bandwidth	The amount of information that something, like a connection to the Internet, can handle in a given time.
Bandwidth Limit	The maximum amount of data per second that a single user is allowed to consume on the wireless network.
Bandwidth Cap	The total amount of data that a user is allowed to consume in a given timeframe before restrictions are applied to that user.
Denial of service	When a machine or network resource is made unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet, typically with malicious intent.
IEEE 802.11a, 082.11b/g/n and 802.11ac and 802.11 ax (Wi-Fi 6)	The IEEE 802.11a, b/g/n, ac and ax protocol is a set of standard specifications for implementing wireless local area network (WLAN) computer communication in the 2.4 and 5 GHz frequency bands. The protocol was created and is maintained by the Institute of Electrical and Electronics Engineers (IEEE).

[1] Devices operating outside the 2.4 GHz and 5 GHz bands include: Ultra low Frequency (ULF); Extremely Low Frequency (ELF); Very Low Frequency (VLF); Low Frequency (LF); Medium Frequency (MF), e.g. Amplitude Modulation (AM) Radio; High Frequency (HF), e.g. cordless phones; Very High Frequency (VHF), e.g. pagers, Frequency Modulation (FM) radio; some Ultra High Frequencies (UHF) like Television (TV), Bluetooth and Microwave; Super High Frequency (SHF), e.g. radar; Extremely High Frequency (EHF) and remote controls

Packet data	A method of transferring data by breaking it up into small chunks called packets. Packet data is how most data travels over the Internet and over cell phone networks.
Peer-to-peer connections (P2P)	A peer-to-peer connection is created when two or more client devices are connected and share resources without going through a separate server computer.
Wi-Fi	A technology for wireless local area networking with devices based on the IEEE 802.11 standards.
Wireless access point	A special-purpose communication device on a wireless local area network that acts as a central transmitter and receiver of wireless radio signals. Wireless access points are most commonly used to support public Internet hotspots and institutional networks where larger buildings and spaces need wireless coverage.
Wireless airspace	The airspace within the University's geographic boundaries in which a whole spectrum of electromagnetic wave frequencies that lie in the range extending from around 3 kHz to 300 GHz may be active.
Wireless client device	Mobile devices such as laptops, tablets, IP phones and other smartphones, or non-portable devices such as desktop computers that are equipped with a wireless network interface.
Wireless client device	A device that operates by connecting to a wireless network.
Staff/Student User/Sponsored Guest	A member of staff or a student that meets the criteria for full time access to the Wireless network and accesses said network via their EMPLID/Portal credentials.
Guest User	A visitor or person who is not a UP staff member or student and self-provisions access to the UP wireless network using private credentials.
Conference User	A visitor or person who is not a UP staff member or student that is attending an event hosted at UP for which the organiser has pre-arranged wireless access.
Eduroam User	A visitor or person who is a member of another educational or research institution that is joined to the eduroam programme and can access the UP wireless network using their home institution's access credentials.

6 Wireless provisioning

6.1 Campus-wide coverage

ITS is responsible for providing, configuring, maintaining and funding a wireless network for use by the whole University community. ITS will strive to provide optimal wireless coverage within resource constraints and priorities.

Priorities for the roll out of wireless coverage funded by ITS will be determined by the IT Director & CIO, considering:

- population density frequenting a space;
- educational/mission-defined needs;
- unstructured spaces;
- cost-effectiveness of technology in specific structure/space, e.g. public service areas, open seating areas, conference rooms, cafés, lounges, general lecture halls and outside meeting spaces.

Provided coverage will not be for the exclusive use of certain groups but will be available to the whole institution's community.

Coverage is only available in certain areas. See http://www.up.ac.za/up-wireless-network/article/277134/wifi-coverage-maps-campus-view for information on wireless coverage.

6.2 Self-funded wireless expansion

Departments and individuals wishing to provide additional wireless access points for their own use and at their own cost must complete and submit a request to extend wireless network coverage via the ITS service catalogue item: self-funded wireless expansion.

The request will be processed as follows:

- The application will be investigated and considered by ITS.
- Recommendations, calculation of costs, etc. will be given as feedback by ITS.
- The financing of the expansion will be covered by the Department or the individual.
- Implementation of recommendations will be coordinated by ITS.
- The Procurement Division must be contacted for procurement of all relevant equipment required.

7 Protection of the wireless airspace

The wireless airspace within the geographic boundaries of the University serves as the transport medium for its wireless technology. It is a resource of the institution that is managed and secured by ITS to ensure a high quality and secure wireless network that interacts optimally with the wired network.

The current wireless network technology used is based upon products that use the frequency bands of 2.4 GHz and 5 GHz and that conform to the IEEE 802.11b/g/n, ac and ax standard. Other wireless products that use the same frequency bands but do not conform to this standard can cause interference with the institution's wireless service and can prevent legitimate users from obtaining or maintaining network connectivity.

To prevent such interference and unauthorised intrusion in the UP wireless airspace, and to ensure the secure configuration of wireless network devices, authorisation by ITS is required for all wireless network devices that can broadcast, send or receive information in the above frequencies.

7.1 Unauthorised wireless network devices

Unauthorised wireless devices are prohibited from connecting with the wireless network as follows:

- Any device such as, but not limited to, wireless access points, routers, Wi-Fi printers or any other electronic device that may interfere with the University's Wi-Fi network.

The administrators of any currently-deployed unauthorised wireless devices must take urgent steps to contact ITS, at help@it.up.ac.za, or (012) 420-3051, to determine whether these devices may be integrated into the institution scheme or must be disconnected.

Those contemplating deployment of wireless-enabled hardware unrelated to networking (alarm systems, projectors, printers, etc.) that operates on the 2.4 or 5 GHz bands should consult with ITS regarding possible impact on the wireless network service.

Other devices, such as 2.4 GHz portable phones and wireless devices using competing wireless technologies (such as certain versions of Bluetooth), that broadcast and receive information on the same frequency as the institution's wireless network, must be avoided.

The institution reserves the right to disable or disconnect any access point or wireless device not installed, configured or approved by ITS. Any user found to have violated these requirements may be subject to disciplinary action.

8 User access to the wireless network

The purpose of the wireless network is to provide access to the Internet and, for authorised users, the UP portals and systems. It is located outside the firewall and access to the internal wired network is not allowed.

The institution provides two levels of access to the wireless network – full and restricted - as stipulated in the table and sections below.

Table 2: Access restrictions

Staff/Student User/Sponsored guest	Bandwidth Limit – 10 Mbps. No bandwidth Cap – 10 GB per 24 hours thereafter bandwidth limit adjusted to 512 kbps.
Guest User	Bandwidth Limit - 2 Mbps Bandwidth Cap – 200 MB per 24 hours
Conference User	Bandwidth Limit – 4 Mbps. No bandwidth Cap – 10 GB per 24 hours thereafter bandwidth limit adjusted to 512 kbps.
eduroam User	Bandwidth Limit – 10 Mbps. No bandwidth Cap – 10 GB per 24 hours thereafter bandwidth limit adjusted to 512 kbps.

Configuration and support information on connecting to the UP wireless network is available on the UP website at http://www.up.ac.za/up-wireless-network.

Peer-to-peer (P2P) connections are not allowed via the institution's wireless network.

All users of the wireless network must adhere to the *Policy on Acceptable Use of Computing Resources* [3] and the *Electronic Communications Policy of the University of Pretoria* [2].

8.1 Staff and student access

Internet access through the TUKS secured Wi-Fi connection is available to registered students, staff members and some sponsored guests of the institution. To acquire full access, users of the wireless network must authenticate their identity with their Portal credentials. A secure networking environment will handle the authentication process and data communication.

8.2 Guest access

Restricted access to the wireless network is available to guests of the University, as well as anyone within wireless coverage on campus.

The access is restricted in that it is given for a limited period only and that bandwidth usage is limited and managed.

Restricted access is also available to conference attendees. Conference organisers must complete and submit a request for such access at their own cost via the IT service catalogue item: Cable / Wireless Network Access for events and conferences.

8.3 Requirements for full access

Full access is available to staff and registered students of the University.

Staff and students from other institutions that participate in the eduroam service may also sign on for full access by using their home institution's credentials to authenticate as eduroam users. (See http://www.up.ac.za/en/it-services/article/256971/eduroam-education-roaming for more information.)

Table 3 below states the requirements for full access.

Table 3: Full access requirements

STAFF	STUDENTS
Person must have an official institutional personnel number.	Person must be a registered student of the institution.
A personal or institution-owned device may be used.	A personal or institution-owned device may be used.
Device must have enabled wireless capabilities.	Device must have enabled wireless capabilities.
Device must support the standard protocol IEEE 802.11a, b/g/n, ac or ax.	Device must support the standard protocol IEEE 802.11a, b/g/n, ac or ax.
Device must run a supported operating system, e.g. Windows 10, supported versions of Android and iOS.	Device must run a supported operating system, e.g. Windows 10, supported versions of Android and iOS.
The latest operating system security updates must be installed on the device.	The latest operating system security updates must be installed on the device.
Device must be virus free.	Device must be virus free.
Device must have an up-to-date anti-virus software, e.g. McAfee.	Device must have an up-to-date anti-virus software, e.g. McAfee.
Device must be within wireless coverage on Campus.	Device must be within wireless coverage on Campus.

Users of the TUKS secured Wi-Fi connection are responsible to ensure that the devices that they use are compliant with these requirements before connecting to the network.

ITS retains the right to check the above requirements and prohibit or prevent access until a device is considered compliant.

9 Monitoring and management of the usage of the wireless network

In a wireless environment, network reliability is a function both of the level of user congestion (traffic loads) and service availability (interference and coverage). ITS strives towards a cost-effective balance between expected use, peak times and technical issues. Adjustments in coverage and capacity may occur from time to time.

Users of the wireless network must take note of the University's right to monitor the flow of electronic communications traffic in order to protect the integrity of the proper and legal operation of its information and communication systems as stipulated in the *Electronic Communications Policy of the University of Pretoria* [2]. Misuse of the wireless network, e.g. the download of illegal content, or copyrighted content without the necessary permission, shall be deemed as misconduct and ITS may initiate appropriate investigation and disciplinary action against such users.

10 Support

ITS support for connecting to the wireless network and support on institution-owned laptops are available within standard business operating times (07:30 – 16:00).

Support is available for staff, between 07:00 and 16:30, Monday to Friday, at the IT Helpdesk at (012) 420-3051 or help@it.up.ac.za.

Support is available for students, between 07:30 and 22:00, Monday to Friday, and 08:00 till 17:00, on a Saturday, at the Student Helpdesk at (012) 420-3837 or studenthelp@up.ac.za.

11 Roles and responsibilities

Roles and responsibilities related to the wireless network are defined below.

11.1 Information Technology Services

- All wireless access points connecting to the institution's network will be surveyed, verified, purchased, documented, installed, configured and managed by ITS personnel.
- Wireless usage will be monitored to gauge bandwidth, system traffic and data transmission levels.
- ITS will determine approved technology, equipment, vendors and configuration.
- ITS is responsible for establishing and maintaining product and protocol standards re wireless data network services.
- ITS is responsible for the expansion and maintenance budget for the centralised infrastructure of the wireless network.
- Exceptions to the conditions/standards may be made by ITS when deemed necessary and do not pose a threat to security.

11.2 Users

- Requirements for wireless coverage and/or mobility on a permanent or ad hoc basis should be timely communicated to ITS.
- Users are responsible for budgeting for expansions and financing of unbudgeted expansions of the wireless network.
- Usage of the wireless network service must comply with the *Policy on Acceptable Use of Computing Resources* [3].

11.3 Responsibility for implementation

The Deputy Director: IT Operations is responsible to ensure that IT Operations Staff implement and maintain the control measures included in this document.

Deans, directors and heads of academic and Professional service departments, as well as student leaders, must take reasonable steps to ensure that all users take note of the contents of this document and comply with it.

12 Liability

The institution cannot be held legally responsible for connection failures, Internet service disruption or denials of service.

13 Associated documents

[1] Information Technology Security Policy
[2] Electronic Communications Policy of the University of Pretoria
[3] Policy on Acceptable Use of Computing Resources

14 Document life cycle

This document should be reviewed every two years, or sooner if required.

Appendix A – ITS documentation control information

Title and synopsis

Title	Wireless Network Standards and Procedures
Synopsis	Standards and procedures to regulate the provisioning and secure use of the wireless data network
Audience	All users of the UP wireless network
Compliance	Compulsory
Keywords	Wireless network, regulations, provisioning, usage, coverage, requirements.
Owner	Sven Pey
Author(s)	Rupert Botha, Sven Pey, Yzelle Roets.
Contributor(s)	Christo van Schalkwyk, Marcel Vladar

Enquiries and requests

IT Helpdesk	Tel: (012) 420 3051 Email: ithelp@up.ac.za
Service Management System	https://upsmax.up.ac.za

Approval list

ITS Policies, Standards and Procedures Committee
Deputy-Director: IT Operations
ITS Senior Management Committee

Record of changes

Date	Edited by	Description
2017/11/20	E Ferreira	Repurposing of the previous Wireless Network Policy document (ADM1180) as a standard and procedures for the wireless network.
2020/08/03	R Botha, M Vladar, C van Schalkwyk	Changes and adding 802.11ax, Wi-Fi limits, etc.
This document must be reviewed biennially or earlier where necessary.		

List of tables

List of abbreviations and acronyms

CIO ..... Chief Information Officer
EMPLID ..... Employee Identification Number
GB ..... Gigabyte
GHz ..... Gigahertz
IEEE ..... Institute of Electrical and Electronics Engineers
iOS ..... iPhone Operating System.
IT ..... Information Technology
ITS ..... Information Technology Service
Kbps ..... Kilobits Per Second
kHz ..... kilohertz
MB ..... MegaByte
Mbps ..... Megabits per second
P2P ..... Peer-to-Peer
PC ..... Personal Computer
PDA ..... Personal Digital Assistant
UP ..... University of Pretoria
WLAN ..... Wireless local area network