POLICY OWNER	:	Information Technology Services			
TITLE	:	Wi-Fi Policy			
Document Code	:	IMU/POL/ITS/09	Edition	:	1
Approval Body	:	Management Committee	Approval Date	:	03/05/17
Effective Date	:	03/05/17	Pages	:	**6**

1.0 OBJECTIVE & BACKGROUND

The objective of this policy is to provide a clear statement to all Users on IMU's Wi-Fi facilities, it's services and their User's responsibilities.

This policy was developed in response to the need for guidelines to describe the acceptable use of Wi-Fi service in International Medical University (IMU) taking into consideration IMU's intention to facilitate and support teaching or academic activities required in the University. Additionally, this policy is to protect the IMU technology-based resources from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, or damage to IMU public image.

2.0 SCOPE

This policy applies to: -

- All Users of IMU Education Sdn Bhd ("IMU"), which is also known as the International Medical University ("University")."

3.0 DEFINITION

No.	Term	Meaning
1	ITS	Information Technology Services
2	University	International Medical University
3	User	Any user who has been authorized by the relevant IMU supervisor/officer to access any IMU print services or IT facility, and includes (but is not limited to) staff of IMU, students, consultants, Visitors, Honorary appointees and Alumni

4.0 RESPONSIBILITY FOR IMPLEMENTATION

No.	Party	Roles & Responsibilities
1	Users	Users are expected to use IT resources in a responsible manner. I.e. users are expected to follow all pertinent Malaysian Laws and IMU policies.
2	ITS	ITS is responsible for the design, operation and management of Wi-Fi network, including provision of security measures at the network level. ITS department shall manage the policy.

5.0 POLICY DETAILS

5.1 Scope

5.1.1 This policy applies to all users in IMU. Users shall be further refined to staff, student and guest of IMU.

5.2 Policy

5.2.1 Wireless "access points," shall be located throughout the classrooms and common areas of all IMU campuses. ITS monitors the AP to ensure connectivity of eighty (80) connections to one (1) AP.

5.2.2 Wi-Fi network is provided to support of teaching or related academic activities to access Campus Network and Internet in lecture theatres, classrooms and libraries. Use of Wi-Fi network for other purposes should be limited and approved by the ITS staff.

5.2.3 IMU's wireless network is also not designed to support latency intolerant applications such as Voice over Internet Protocol (VoIP) over Wi-Fi. The wireless network should be used primarily for general functions such as Web browsing and email. It is not designed to efficiently support high-bandwidth applications such as, but not limited to, streaming media or large file transfers.

5.2.4 Wireless bandwidth is shared by everyone connected to a given wireless Access Point (AP). As the number of wireless connections increase, the bandwidth available to each connection decreases and performance may deteriorate. Applications that generate high network traffic do not work well on wireless networks and negatively impact performance for everyone connected to the same access point.

5.2.5 Wi-Fi network users should ensure their computer systems are properly configured and operated so that they do not cause inconveniences to other Wi-Fi network users and the campus network users.

5.2.6 Wi-Fi network users should get their network addresses automatically; a valid network address will be granted when connected.

5.2.7 ITS reserves the right to prohibit the running of other servers which are harmful to the network (e.g. system services such as DHCP).

5.2.8 Use of other network address is prohibited. Setting up routing or other special network functions is prohibited.

5.2.9 Setup of servers set up for the provision of ftp/web/vnc/telnet/ssh services are prohibited. ITS shall request that any application that uses more than fifty (50) percent of a shared radio channel on a consistent basis be moved to a wired connection.

5.2.10 In the event that a Wi-Fi network connected device presents an immediate security risk to equipment, software or data in campus network, ITSC staff has the right to terminate this connection without prior notice.

5.2.11 ITS shall provide notice of Wi-Fi network unavailability due to regular maintenance, upgrades or changes. However, in the event of an emergency, ITS shall shut down partial or whole Wi-Fi network with little or no advance notification.

5.3 User Responsibilities

5.3.1 Users are responsible for use in a manner that is ethical, legal, and not to the detriment of others.

5.3.2 Users are responsible for all activities initiated from their computer.

5.3.3 Users shall ensure and/or take steps to:

- Reduce excessive network traffic such as broadcasting and sending massive messages and unsolicited emails;
- Do not set up routing or other special network functions;
- Under take developing networking software;
- Do not share their accounts.

5.3.4 Users are responsible for the licenses of the software installed in their devices connecting to the network.

5.3.5 ITS reserves the right to temporary or permanent revoke access of the user's device without making prior notice to the user. This is to prevent severe network problem(s) which may arise from the Wi-Fi network user's computer system.

5.3.6 Offences which are in violation of law usually shall result in immediate loss of access privilege of Wi-Fi network and will be reported to the appropriate University or law enforcement authorities.

5.3.7 The use of personal Wi-Fi access points (APs) can interfere with and/or slow the wireless connection of users in close proximity. For this reason, personal Wi-Fi access points or routers are not allowed. ITS shall continuously conduct sweeps of the wireless network to ensure there are no personal access points are present.

5.3.8 Minimum requirements and Supported Technology

5.3.9 All devices, regardless of location or ownership, must satisfy the following minimum network connectivity requirements, as appropriate, before connecting to the campus network. Devices known to be vulnerable, to present a security risk, or to be infected with malicious software must not be connected to the campus network or to devices on the campus network. Devices not meeting these requirements, as well as devices found to be disruptive to the operation of the campus network, are subject to being blocked or disconnected.

5.3.10 IMU uses the 802.11n and 802.11ac protocols as its wireless network standards, transmitting in the 2.4 GHz and 5 GHz radio frequency spectrums.

5.3.11 Users are advised to set their devices to 5GHz frequency where applicable over 2.4 GHz.

5.3.12 ITS managed the Service Set IDentifier (SSID) within IMU premises. These SSID are:

S/N	SSID	Description
1	Staff @ IMU	Staff access. Unlimited access to devices and access governed by Active Directory. Access shall be reset on one (1) day basis
2	Student @ IMU	Student access. Limited to three (3) devices. Access shall reset on one (1) day basis
3	Guest @ IMU	Access via Captive Portal an access shall be reset on a four (4) hour basis. Password shall be updated every quarter.
4	Guest @ Healthcare	Access shall be reset on **ten (10) minutes of inactivity**. Password shall be updated every quarter.

5.3.13 User can request of Wi-Fi use for specific event. This shall be reviewed by ITS and when approved, an SSID with limited period for the event shall be created.

5.3.14 All Wireless devices come from the factory with standard applications. ITS may or may not be familiar with these standard set of applications due to the constant changing development that occur with wireless devices in general. Support for these standard applications is on a best effort basis.

5.3.15 IT supports Microsoft Office 365 and Timetable Management System (TiMS). Third party applications are not supported

6.0 RELATED LEGISLATION

-

7.0 RELATED POLICY

-

8.0 REVIEW

The Policy will be reviewed at least once every three (3) years, and if necessary, updates will be made to reflect changes on regulatory and compliance guidelines.

Appendix A: Design Standards:

To ensure appropriate and effective wireless coverage for all areas, design standards were developed in coordination with the University's wireless vendor. These standards are applied to various University use cases to accomplish Wi-Fi coverage goals.

NO	DESIGN STANDARD	EXPECTED USER DENSITY	BANDWIDTH EXPECTATIONS
a.1	Hostel residence	Low	General Web traffic, 360 fps streaming audio/video.
a.2	General office space	Low	
a.3	Open collaborative space	Medium	General Web traffic, 760 fps streaming audio/video.
a.4	PBL, Classrooms	Medium	
a.4	Auditorium, Lecture Theaters, Senate, Boardroom.	High	General Web traffic, 760 fps streaming audio/video. 30-40 user connections per AP.