Guidelines for IIUM Campus Network and Telephone Services - *DRAFT*

IIUM ICT GUIDELINES

PREPARED FOR:
International Islamic University Malaysia

PREPARED BY:
Information Technology Division

Document Change Log

Release Version	Date	Pages Affected	Remarks/Change Reference
Version 1.0	15/10/2024	All	New formulated guideline. Combination of network and telephone in one guideline.

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Ahmad Naim bin Hamat	Approval by ITD Management Meeting No.16/2024	22/10/2024	30/10/2024
Shahidah binti Mahbob	New formulated content of the new guideline for review	28/10/2024	

1. OBJECTIVE

This objective of this guideline is to establish policies and procedures for IIUM network and telephone services, ensuring **secure, reliable, and controlled** access.

2. TERMS AND DEFINITIONS

Term	Definition
IIUM	The International Islamic University Malaysia, otherwise known as "the University"
ICT	Information and Communication Technology
CDIO/CIO	Chief Digital Information Officer / Chief Information Officer
ITD	Information Technology Division
ITD Management	CDIO/CIO, Director, Senior Deputy Directors, Deputy Directors and Team Leaders of ITD.
Staff	Permanent Staff and Contract Staff of IIUM.
External party	Guest or visitor.
Network-connected	All devices that are connected by wire, optical cables or wireless to the digital telecommunication networks that are owned and/or operated by the University.

3. POLICY STATEMENTS

3.1 IIUM Network Services

3.1.1 Wired Network Services

(i) All staff and matriculated students are entitled to access the University wired network.

(ii) External parties may be granted restricted network access via wireless.

3.1.1.1 Access Eligibility

(i) All staff and matriculated students are entitled to access the University's wired network.

(ii) External parties may be granted restricted network access via wireless.

3.1.1.2 User Responsibility

(i) Users must comply with network policies and ensure the security of their credentials.

(ii) Users are responsible for all activities performed using their network accounts.

3.1.1.3 Network Management

(i) The University reserves the right to revoke or limit access if misuse is detected.

3.1.2 Wireless Network Services

3.1.2.1 Access & Authentication

(i) Wireless services are available for all IIUM staff and students.

(ii) Staff must use the "IIUM-Staff" SSID; students must use "IIUM-Student" SSID.

(iii) External guests shall use "IIUM-Guest" with restricted access.

(iv) Eduroam is available for international academic users.

(v) Authentication requires official IIUM credentials:

(vi) Staff: username: <email username>, password: <email password>

(vii) Student: username: <matric number>, password: <imaalum password>

(viii) Credential sharing is strictly prohibited and will result in disciplinary action.

3.1.2.2 Network Support & Device Compatibility

(i) ITD provides support only for devices with supported operating systems, including:

- iOS 16+, iPadOS 16+, Android 12+, Windows 10/11, macOS 13+

(ii) Devices using outdated operating systems will not receive support.

3.1.2.3 Coverage & Restriction

(i) Wireless access is available across campus, including libraries, lecture halls, hostels (Mahallah), and common areas.

(ii) Some remote areas may have limited connectivity.

(iii) Illegal activities (e.g., hacking, unauthorized content sharing) are strictly prohibited.

3.1.2.4 Network Security & Fair Usage Policy

(i) Personal routers, access points, or network devices are strictly prohibited due to security risks. Unauthorized devices will be disconnected and confiscated.

(ii) Users must ensure device security (update software, use strong passwords, avoid phishing attempts).

(iii) A Fair Usage Policy (FUP) is enforced to prevent network congestion. High-bandwidth activities (e.g., large downloads, streaming, P2P file sharing) should not degrade network performance.

(iv) Academic and research traffic will receive priority over non-essential activities (e.g., gaming, social media).

(v) IIUM reserves the right to block or throttle non-academic traffic when necessary.

3.1.2.5 Wireless Performance & Compliance

(i) Allowed bandwidth speed: Up to 100 Mbps for students in Mahallah to ensure an optimal user experience.

(ii) Only 802.1x enterprise authentication and captive portal methods are supported.

(iii) Wireless access must be used exclusively for educational, research, and beneficial purposes.

4. Compliance & Enforcement

4.1 Monitoring & Auditing

(i) Network activities will be monitored for security and compliance with ISO/IEC 27001:2022.

(ii) Logs and access records will be maintained as part of incident response and risk management.

4.2 Enforcement & Disciplinary Actions

(i) Violations of this guideline may result in temporary or permanent suspension of network access.

(ii) Severe breaches (e.g., unauthorized access, hacking, network abuse) will be reported for disciplinary and/or legal action.

4.3 Periodic Review

4.3.1 This guideline will be reviewed annually to ensure compliance with ISO 27001:2022 and evolving security requirements.

4.3.1.1 All staff and matriculated students of IIUM are entitled to have access to the University's network.

4.3.1.2 External party of the University shall be given network access via wireless connection with restricted usage time.

4.3.1.3 All IIUM network users shall agree to adhere to the rules and regulations applied to the network.

4.3.1.4 Users are responsible for any activity on his/her network account.

4.3.1.5 The University reserves the right to revoke the network connections whenever deem necessary.

4.3.2 Wireless Services

4.3.2.1 IIUM wireless is eligible for all IIUM's Staff and Students.

4.3.2.2 All IIUM staff need to use "IIUM-Staff" SSID, and all IIUM student need to use "IIUM-Student" SSID.

4.3.2.3 There are four SSID in IIUM which: IIUM-Staff, IIUM-Student, IIUM-Guest

and Eduroam.

4.3.2.4 All staffs and students must authenticate using their own IIUM credentials to access wireless services. The credentials are strictly for own use only and any sharing of credentials may lead to disciplinary action.

4.3.2.5 ITD will only provide troubleshooting support for devices running operating systems and hardware that are supported by the manufacturer. This includes, but is not limited to, the following:

- iOS: Devices running iOS 16 and above
- iPadOS: Devices running iPadOS 16 and above
- Android: Devices running Android 12 and above
- Windows: Devices running Windows 10 and Windows 11
- MacOS: Devices running MacOS 13 Ventura and above

Devices running older versions, such as iOS 15, iPadOS 15, Android 11, Windows 7, or MacOS 12 Monterey, are not eligible for support, as they no longer receive security updates from their respective manufacturers.

4.3.2.6 The wireless network is available throughout the campus, including Kuliyyah, libraries, lecture halls, Mahallah and common areas. Some remote or low-traffic areas may have limited coverage.

4.3.2.7 The IIUM wireless network must not be used for illegal activities, such as hacking, distributing copyrighted material without permission, or accessing offensive content. Violations may result in disciplinary action, including suspension of network access.

4.3.2.8 It is illegal for users to connect personal routers, access points, or any other network devices to the IIUM network. These unauthorised devices can cause network interference and pose security risks. Violations of this guideline will result in the immediate disconnection and confiscation of the device and possible disciplinary action.

4.3.2.9 All users must adhere to a fair usage policy, ensuring that network resources are shared equitably. Activities such as large file downloads,

video streaming, or peer-to-peer (P2P) file sharing should not degrade the performance of the network for others. IIUM have right to capped or blocked website that not relevant to teaching and learning.

4.3.2.10 IIUM will prioritise network traffic for academic services, research, and educational resources. Non-essential traffic, such as gaming or social media, may experience lower priority, especially during peak academic hours.

4.3.2.11 IIUM Students and staff are responsible for the security of their own devices. This includes maintaining up-to-date software, using strong passwords, and avoiding risky online behaviours that could compromise their device or the network.

4.3.2.12 Users shall enter username and password for credential requirement as follows:

- **Staff**: username: <*email username* >, password: <*email password*>
- **Student**: username: <*matric number*>, password: <imaalum *password*>

4.3.2.13 IIUM only support 802.1x enterprise and captive portal for user authentication.

4.3.2.14 Student are advised to use the Wi-Fi services for the education, research and beneficial purposes only.

4.3.2.15 Allowed bandwidth speed is up to 100 Mbps for better user experience among the students in the Mahallah.

4.4 IIUM Telephone Services

4.4.1 Outgoing Call Entitlement

Users	Category (Outgoing)
Senior Officers	
Rector, Deputy Rectors & Deans, Executive Directors, and respective secretaries.	7
Deputy Deans/Directors & Heads of Departments and respective Personal Assistants.	5
Academic Staff	
Academic Fellows	4
Professors/ Associate Profs.	4
Assistant Profs.	4
Lecturers/ Teachers	3
Assistant Lecturers	3
Administrative Staff	
Category A (Professional & Management Group)	4
Category B (Support Group)	3
Category C (Support Group)	3
General Number of Kulliyyah/Centre/Division	1
Facsimile Line (Main Office)	6
Facsimile Line (Department Office)	3
Other entities	
Student Society	1
Laboratories	1

Table 1: Call categories

Please refer to Table 2 below for further information.

Category	Destination
1	Internal calls only (intra and inter-campus)
2	Local calls only
3	Local and state
4	Local/State and Handphone
5	Peninsular Malaysia
6	Peninsular Malaysia, Sabah & Sarawak
7	International Access

Table 2: Call categories and their definitions

4.4.2 Telephone Use/Access

4.4.2.1 Telephone facilities for students' societies, computer laboratories, and Kuliyyah`s laboratories are restricted to internal calls only.

4.4.2.2 All applicants for telephone services shall submit at the ICT service desk counter or email to servicedesk@iium.edu.my.

4.4.2.3 Staff may bring their physical telephone with them when they transfer or move to another location.

4.4.2.4 Staff who has tendered their resignation or has been terminated by the University must follow the MSD Staff clearance procedure in order to ensure that telephone services are disconnected and the peripherals collected by ITD.

4.4.3 Telephone Entitlement Facilities

The telephone entitlement of facilities for staff is as depicts in Table 3 below:

Users	DID (Direct Incoming)	Voice mail
Senior Officers		
Rector, Deputy Rectors & Deans, Executive Directors and their respective secretary	Y	Y
Deputy Deans/Directors & Heads of Departments and their respective secretary	Y	Y

Academic Staff		
Professors/ Associate Profs.	Y	Y
Assistant Profs.	Y	Y
Lecturers/ Teachers	Y	Y
Assistant Lecturers	N	Y
Administrative Staff		
Category A	Y	Y
Category B*	N	Y
Category C	N	Y
General Number of Kulliyyah/Centre/Division	Y	N
Facsimile Line	Y	N
Other Entities		
Student Society	Y	N
Laboratories	Y	N

Table 3: Telephone entitlement facilities

*Except for Executive Officer (N27) and Assistant Accountant (W29) at respective Kulliyyahs/Centres/Divisions with the recommendation from the Dean/Director and approval by Director of ITD.

5. IMPLEMENTATION AND NON-COMPLIANCE

5.1 The Director of ITD holds the responsibility for the implementation of this guideline and shall take necessary actions in the event of violation of this guideline.

5.2 This guideline is applicable to the University community and any infringement of the guideline may subject to disciplinary actions and any other actions deem necessary.

6. ENFORCEMENT

6.1 This guideline is applicable to the University community and any infringement of the guideline may subject to disciplinary actions and any other actions deem necessary.

6.2 This procedure shall be implemented in accordance with IIUM's ICT Security Procedure in compliance with ISO/IEC 27001:2022 requirements to ensure confidentiality, availability, and integrity in all processes. All processes, decisions, and activities under this policy/guideline must uphold the principles of confidentiality, availability, and integrity to protect the information, data, and assets.

7. MAINTENANCE OF THE GUIDELINES

The Information Technology Division is responsible for the formulation and maintenance of this guideline.

8. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

This guideline shall be read together with the following or any documents which recently approved:

8.1 Policy for Service desk and Incident management.

8.2 IIUM ICT Policy

8.3 ICT Regulations

8.4 IIUM Information Management Policy

8.5 IIUM ICT Security Procedure

8.6 IT Infrastructure Library (ITIL)

8.7 Control of Business IT (COBIT)

8.8 Procedure of IT Service Request