Guidelines for IIUM Campus Network and Telephone Services

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 guidelines formulated. Combination of network and telephone in one guideline.
Version 1.0	25/06/2025	-	Endorsement from ITD Management

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	
Noor Helmi Mokhtar	New formulated content of the new guideline for review according to the ISO/IEC 27001:2022 requirements	26/03/2025	
Noor Helmi Mokhtar	Endorsement from ITD Management	23/06/2025	25/06/2025

1. OBJECTIVE

The 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 Access Control

3.1.1 User Authentication & Authorization

(i) Only **authorized staff, students, and registered guests** can access IIUM network services.

(ii) Authentication must use **official IIUM credentials**:

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

(iii) **Multi-Factor Authentication (MFA)** is required for accessing critical university resources.

(iv) **Guest users** must register for temporary access via **"IIUM-Guest"** SSID.

(v) Access levels are assigned based on **roles and responsibilities** (Least Privilege Principle).

3.1.2 Accountability & Restrictions

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

(ii) **Failed login attempts** are monitored, and accounts will be locked after multiple failures.

(iii) **Inactive accounts exceeding 6 months** will be deactivated.

3.2 IIUM Network Services

3.2.1 Wired Network Services

(i) Wired network services are available for **all staff and students** with **registered IIUM credentials**.

(ii) External parties shall have **restricted wired access** only where necessary.

(iii) **Network activities are monitored** for compliance and security.

3.2.2 Wireless Network Services

3.2.2.1 Network Segmentation

(i) Staff SSID: **"IIUM-Staff"** (Internal and External Access)

(ii) Students SSID: **"IIUM-Student"** (Internal and External Access with restricted access)

(iii) Guests SSID: **"IIUM-Guest"** (Limited access)

(iv) Visitors for Other Universities SSID: **"eduroam"** (External Access with restricted Internal access)

(v) Personal hotspots or unauthorized access points **are prohibited**.

3.2.2.2 Security & Compliance

(i) **Only devices with updated operating systems** are supported (Windows 10/11, macOS 13+, Android 12+, iOS 16+).

(ii) **Unpatched or outdated devices** will be denied network access.

(iii) Users are responsible for maintaining **device security** (firewalls, antivirus, software updates).

3.2.2.3 Usage Restrictions & Fair Usage Policy

(i) **Illegal activities** (hacking, unauthorized content distribution, accessing offensive material) are strictly prohibited.

(ii) Network traffic is **monitored and prioritized** for academic and research purposes.

(iii) **High-bandwidth activities** (e.g., gaming, streaming, torrents) will be **throttled or blocked** during peak hours.

3.3 IIUM Telephone Services

3.3.1 Fixed-Line & IP Telephony Services

(i) IIUM provides **telephone services** for staff, faculty, and authorized departments for **academic and administrative purposes**.

(ii) Telephone extensions are assigned by **ITD Management** based on **departmental needs**.

(iii) Calls made using IIUM telephone services are **monitored and logged** for security and operational efficiency.

(iv) Unauthorized use of IIUM telephone services for **personal, commercial, or fraudulent activities** is strictly prohibited.

3.3.2 Telephone Access & Restrictions

3.3.2.1 Internal Calls

(i) Staff members can make **internal calls** without restrictions.

3.3.2.2 External Calls

(i) **Local and international calls** require prior authorization from **ITD Management**.

3.3.2.3 Voicemail & Call Forwarding

(i) Voicemail services are available for **authorized extensions.**

(ii) Call forwarding is allowed only to **register IIUM numbers.**

3.3.2.4 Entitlement

(i) Users outgoing call Category shall be referred to **Table 1**.

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*

(ii) The definition of the Outgoing Call Category is described in **Table 2**.

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*

(iii) The entitlement for Direct Incoming Calls and voice mail services is described in **Table 3**.

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 KCDIOM	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 KCDIOM with the recommendation from the Dean/Director and approval by the Director of ITD.*

3.3.3 Telephone Security & Compliance

3.3.3.1 Confidentiality & Privacy

(i) Users must ensure that **sensitive or confidential discussions** are conducted securely.

(ii) Recording calls **without prior consent** is prohibited.

3.3.3.2 Spam & Unsolicited Calls

(i) IIUM reserves the right to **block spam or scam calls** for security reasons.

3.3.3.3 Physical Security of Phone Devices

(i) Unauthorized removal or tampering with IIUM telephone equipment **is prohibited**.

(ii) Damaged or faulty devices must be **reported to ITD** immediately.

3.4 Asset Management

3.4.1 Inventory of Network Assets

(i) All network devices (routers, switches, servers) **must be inventoried and labeled.**

(ii) Unauthorized IT assets **must not be connected** to the IIUM network.

3.4.2 Third-Party and Vendor Access

(i) External service providers require **formal approval and signed agreements** for network access.

(ii) Vendor access is **limited to pre-defined maintenance periods.**

3.5 Cryptographic Control

3.5.1 Encryption Standards

(i) Sensitive data transmitted over IIUM networks **must be encrypted** (TLS 1.2+, WPA3 for Wi-Fi).

(ii) **End-to-end encryption (E2EE)** is required for critical university communications.

3.5.2 Password & Key Management

(i) Passwords **must be complex and changed regularly** (minimum 12 characters, mix of letters, numbers, and symbols).

(ii) **Cryptographic keys** must be stored securely and **rotated periodically**.

3.6 Physical & Environmental Security

3.6.1 Securing Network Infrastructure

(i) Network rooms, data centers, and wiring closets **must be access-controlled**.

(ii) Surveillance cameras should monitor **critical network infrastructure**.

3.6.2 Environmental Controls

(i) Data centers must have **fire suppression systems, temperature control, and UPS backup**.

(ii) Unauthorized personnel **must not access network equipment**.

3.7 Operational Security

3.7.1 Monitoring & Logging

(i) **All network activities are logged and monitored** for security threats.

(ii) Logs must be retained for **at least 12 months**.

(iii) **Automated intrusion detection (IDS/IPS) systems** are in place to prevent attacks.

3.7.2 Incident Response & Recovery

(i) Network security incidents must be **reported immediately** to **IIUM CSIRT**.

(ii) **Regular security audits** will be conducted to identify vulnerabilities.

(iii) A **Business Continuity Plan (BCP)** ensures network resilience in case of disruptions.

3.8 Communication Security

3.8.1 Securing Network Communications

(i) Network data must be **transmitted securely** using **VPN, TLS, and WPA3** for wireless connections.

(ii) **Unsecured protocols (e.g., HTTP, Telnet, FTP)** are **not permitted**.

4. COMPLIANCE & ENFORCEMENT

4.1 Monitoring & Auditing

(i) **All network traffic is monitored** to detect suspicious activities.

(ii) Regular **security assessments** are performed to ensure compliance with **ISO 27001:2022**.

4.2 Enforcement & Disciplinary Actions

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

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

4.3 **Periodic Review**

(i) The guidelines will be reviewed **annually** to incorporate security improvements.

5. IMPLEMENTATION AND NON-COMPLIANCE

5.1 The Director of ITD is responsible for the implementation and enforcement of this guideline. In case of violations, necessary corrective actions, including suspension, revocation, or disciplinary measures, shall be taken.

5.2 This guideline applies to all members of the University community. Any non-compliance may result in disciplinary actions, including but not limited to:

- Temporary or permanent revocation of network/telephone access
- Disciplinary actions under university regulations
- Legal actions for severe violations

6. ENFORCEMENT

This guideline is mandatory for all IIUM users. Any infringement of the guidelines will be subject to investigation and enforcement actions by ITD in collaboration with relevant University authorities.

7. MAINTENANCE OF THE GUIDELINES

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

8. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

This guideline shall be read together with the following or any documents as below:

8.1 ICT Regulations

8.2 IIUM ICT Security Procedure

8.3 Policy for Responsible Use of ICT Resources

8.4 Related IIUM ICT Policies