GUIDELINES ON BRING YOUR OWN DEVICE (BYOD) USAGE -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	25/06/2025	-	Endorsement by ITD Management
Version 2.0	/2025	-	Endorsement by ITD Management

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Muhammad Izzat bin Mohd Bahamam	Endorsement from ITD Management	23/06/2025	25/06/2025
Muhammad Izzat bin Mohd Bahamam	Submission to ITD Management	28/10/2025	

1. OBJECTIVE

The objective of this document is to define the guidelines for the usage of personal devices, including computers and other computing devices, by IIUM staff and students. It also outlines security requirements, access policies, and record-keeping procedures to ensure compliance with institutional IT policies.

2. SCOPE

2.1 This policy applies to all IIUM staff and students, including full-time, part-time, and contract employees, as well as all enrolled students who use personal devices to access University resources.

3. TERMS AND DEFINITIONS

Term	Definition
ITD	Information Technology Division
IIUM Staff	Permanent Staff and Contract Staff of IIUM
IIUM Student	"Student" includes any undergraduate student, postgraduate student, part-time student, student under distance learning or off-campus programme, diploma student, matriculation student, exchange and nongraduating student of the University;
BYOD (Bring Your Own Device)	The practice of using personal devices such as laptops, smartphones, tablets, and other computing devices to access IIUM's network and resources.

4. GUIDELINES

4.1 This guideline shall be implemented in accordance with IIUM's Anti-Bribery Management System (ABMS) in compliance with ISO 37001:2025 requirements to ensure transparency, integrity, and accountability in all processes. All processes, decisions, and activities under this guideline must uphold the principles of integrity, transparency, and accountability, and shall be free from any form of bribery or corruption.

4.2 This guideline 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 guideline must uphold the principles of confidentiality, availability and integrity as to protect the information data and assets.

4.3 BYOD users at IIUM must adhere to the following guidelines:

4.3.1 All levels of official IIUM information are considered the property of the University.

4.3.2 Any official materials uploaded, distributed, or shared must have prior approval from the Head of Department.

4.4 BYOD users are strictly prohibited from:

4.4.1 Accessing, storing, or sharing classified Information with unauthorized parties.

4.4.2 Engaging in personal activities on BYOD that may disrupt work productivity.

4.4.3 Using BYOD as a backup medium for storing official information.

4.4.4 Recording official communications or documents for personal use without prior authorization.

4.4.5 Utilizing BYOD as an access point to connect to the IIUM network.

4.31 BYOD users must implement the following security measures to safeguard their devices:

4.3.1 Enable access control mechanisms and ensure the device automatically locks when not in use.

4.3.2 Implement encryption and/or secure protection for folders containing official IIUM information stored on BYOD devices.

4.3.3 Download applications only from authorized and legitimate sources.

4.3.4 Ensure BYOD devices are equipped with the following standard security features:

- Up-to-date antivirus software to protect against malware threats.
- Regularly updated patches and security updates to address vulnerabilities.

4.4 BYOD users must adhere to the following responsibilities:

4.4.1 Use BYOD devices responsibly and comply with all relevant IIUM policies, regulations, and guidelines.

4.4.2 Delete all official IIUM information from the device in cases of service termination, service cancellation, retirement, or when sending the device for maintenance or servicing.

4.4.3 Be accountable for any misuse of BYOD that results in the loss, damage, or exposure of official IIUM information, and may face disciplinary action accordingly.

4.4.4 Acknowledge that IIUM is not liable for any loss or damage of data stored on BYOD devices used for official purposes.

4.4.5 Recognize that mobile devices owned by IIUM are not subject to this policy but must adhere to existing University security protection measures.

5. IMPLEMENTATION AND NON-COMPLIANCE

The Director of ITD is responsible for the implementation of this guideline and ensuring compliance with BYOD policies. Any violation of this guideline may result in actions deemed necessary by ITD, including restricted access to IIUM's network, disciplinary measures, or other corrective actions in accordance with university regulations.

6. ENFORCEMENT

This guideline applies to all members of the IIUM community, including staff and students. Any infringement of this guideline may result in disciplinary actions as per university regulations. Additional actions may be taken as deemed necessary by the ITD, in coordination with relevant University authorities, reserves the right to enforce these measures to protect IIUM's digital infrastructure and ensure responsible use of personal devices.

7. MAINTENANCE OF GUIDELINES

The Information Technology Division (ITD) is responsible for the formulation, periodic review, and maintenance of these guidelines to ensure they remain relevant and effective. Updates may be made as necessary to address emerging security threats, technological advancements, or changes in university policies.

8. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

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

8.1 IIUM ICT Policy
8.2 ICT Regulations
8.3 Information Management Policy
8.4 IIUM ICT Security Procedure
8.5 IT Infrastructure Library(ITIL)
8.6 Control of Business IT(COBIT)