# Guidelines On Bring Your Own Device (BYOD) Usage

International Islamic University Malaysia (IIUM)

## *Document Change Log*

| Release Version | Revision | Date | Pages Affected | Remarks/Change Reference |
|---|---|---|---|---|
| Version 01 | 00 | 25/06/2025 | - | Endorsement by ITD Management |
| Version 02 | 00 | 14/07/2026 | 4,5 & 7 | **Amend Clause 4.1, 4.2, 4.3 and Related Policies/Standards/Procedures/Guidelines** |

## *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 | Endorsement by ITD Management | 14/07/2026 | 14/07/2026 |

## 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 BYOD users at IIUM shall adhere to the following guidelines:

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

4.1.2 All personal devices accessing the University resources through WIFI must be authenticated. For wired access, it must be requested through ITD Servicedesk.

4.1.3 Personal devices shall only be used to access authorized IIUM resources, including IIUM email, Learning Management Systems

(LMS), University applications, official collaboration tools, and publicly available institutional resources.

4.1.4 Users shall store University-related information only in approved institutional storage solutions and shall keep personal information in separate personal storage environments.

**4.2 BYOD users are strictly prohibited from:**

4.2.1 Accessing, copying, storing, or sharing IIUM information beyond their assigned responsibilities or authorized purposes.

4.2.2 Sharing IIUM information with unauthorized individuals or external parties.

4.2.3 Bypassing or attempting to bypass IIUM security controls, policies, or authentication mechanisms.

4.2.4 Transmitting IIUM information over unsecured networks.

4.2.5 Allowing unauthorized individuals to access IIUM information, systems, or personal devices used to access University resources.

4.2.6 Using personal devices in a manner that compromises the security, integrity, or availability of IIUM information, systems, or networks.

4.2.7 Engaging in harassment, discrimination, or any conduct that violates the IIUM Code of Ethics.

**4.3 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 Download and install applications only from legitimate sources.

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

a. Personal devices shall have installed and up-to-date antivirus software to protect against malware
b. 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.

## 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 Policy
8.5 Guidelines on Data Request and Distribution
8.6 Guideline on Information Classification and Labelling
8.7 Guideline for Responsible Use of ICT Resources

| | | |
|---|---|---|
| Title of Guideline | : | Guidelines On Bring Your Own Device (BYOD) Usage |
| Number of Guideline | : | IIUM-ISMS-L3-006 |
| Approving Authority | : | ITD Management |
| Approval Date | : | 14/07/2026 |
| Effective Date | : | 14/07/2026 |
| Version No. | : | 02 |
| Revision No. | : | 00 |