



الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يُونِيسَيتِي إِسْلَامْ أَنْتَارَا بَغْسَا مِلْدِسِيَا
Garden of Knowledge and Virtue

Policy on Website, Web Application and Web Hosting

International Islamic University
Malaysia (IIUM)

Document Change Log

Version	Revision	Revision Date	Pages Affected	Remarks/Change Reference
Version 01	00	26/2/2020		
Version 01	01	26/10/2025	5,7	Update clause 4.1 & 4.2
Version 01	02	04/02/2026	4,5,6,7	Update clause 4.5, 4.8,4.9,4.10,4.11
Version 02	00	07/04/26		Revision of Policy content
Version 02	00	10/04/26		Fair copy of the Policy

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Adis Nabawi, ITD	Initial draft	12/3/2020	
Abu Hurairah A. Manaf	Submission to ICT Committee No. 01/2020	20/10/2022	20/10/2022
Abu Hurairah A. Manaf	Submission to ICT Committee No. 03/2025	28/11/2025	
Abu Hurairah A. Manaf	Submission to ICT Committee No. 01/2026	10/04/2026	
Abu Hurairah A. Manaf	Submission to ICT Committee No. 02/2026	24/09/2026	24/09/2026

SECTION 1: INTRODUCTION

1.1 Objective

The objective of this policy is to establish a robust governance, risk management and control frameworks for International Islamic University Malaysia Websites, Web Applications and Web Hosting; to ensure the data transmitted or stored via the web platforms is protected; to reduce exposure to common web threats; and to comply with applicable laws related to cybersecurity, content regulation and data protection.

1.2 Scope

The scope of this policy covers all items related to the website, web application, and web hosting, hosted, operated, or managed by the University.

1.3 Applicability

Apply to all KCDIOM that host, operate or manage websites, web applications, and web hosting, hereinafter referred to as 'Owner'.

1.4 Terms and Definitions

Term	Definition
Authorised Third Party	Any external individual or organisation formally granted permission to access or use the University's electronic accounts, ICT systems, data, or services for a defined purpose, including but not limited to contractors, consultants, visiting academics, researchers, service providers, and official partners, in accordance with applicable policies, agreements, and security requirements.
CDO	Chief Digital Officer
ICT	Information and Communication Technology
ITD	Information Technology Division
ITD Management	Director, Senior Deputy Directors, Deputy Directors and Team Leaders
KCDIOM	Kulliyyah, Centre, Divisions, Institutes, Offices and Mahallah
User	Any individual or entity, including staff, students, vendors, and other authorised third parties, who access or use the University's ICT facilities.
University/IUM	Means International Islamic University Malaysia
Websites	Means a collection of related web pages containing images, videos or other digital assets. A website is hosted on at least one web server, accessible via a

	network such as the Internet or a private local area network through an Internet address
Web applications	Software applications that are accessed through a web browser over a network, typically the Internet or an internal network, are designed to deliver services or perform functions for users without requiring installation on a local device.
Web hosting service	A service that provides the infrastructure and resources required to store, manage, and make websites or web applications accessible over a network, typically the Internet.

SECTION 2: POLICY STATEMENTS

- 2.1 This policy ensures that all websites, web applications, and web hosting environments are developed, operated, and maintained in a secure, reliable, and compliant manner. IIUM is committed to protecting the confidentiality, integrity, and availability of its digital platforms, safeguarding stakeholder information, and maintaining resilience against cyber threats and operational disruptions. All personnel and service providers shall adhere to the mandatory standards set forth in this policy.
- 2.2 This policy shall be implemented in compliance with the IIUM's Anti-Bribery Management System (ABMS) in accordance with ISO 37001:2025 requirements, to ensure transparency, integrity, and accountability in all processes. All procurement activities shall reflect a commitment to fostering an anti-bribery culture, recognising and managing conflicts of interest, and applying enhanced due diligence to third parties and sustainability-related aspects. Any actual or suspected bribery, corruption, or conflict of interest shall be reported through secure and protected channels, with whistle-blower protections in place.

- 2.3 This policy shall be implemented in accordance with IIUM's ICT Security Policy 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 must uphold the principles of confidentiality, availability and integrity as to protect the information data and assets.

SECTION 3: IMPLEMENTATION OF THE POLICY

3.1 General Requirement

- 3.1.1 All websites, web applications and web hosting services related to IIUM must be hosted under IIUM Hosting. Any exception is subject to approval from the ITD Director.
- 3.1.2 All websites, web applications, and web hosting services that involve a third party must be recommended by ITD before proceeding with the implementation.
- 3.1.3 All websites, web applications and web hosting services hosted by IIUM shall only be used for official purposes. Any exception is subject to the written approval from the ITD Director.
- 3.1.4 All websites must adhere to the Guidelines on IIUM Website Development and Web Content.

3.2 Website Content and Management

- 3.2.1 All KCDIOM that host, manage and operate websites must ensure that information published is accurate, up-to-date, and complete.
- 3.2.2 The content on websites that are no longer in use or has reached the end of its lifecycle should be archived accordingly subject to the Guidelines on IIUM Website Development and Web Content.

3.3 Prohibited Content

- 3.3.1 No person shall create, publish, share or make available within or through the websites, web applications or web hosting hosted by IIUM, the following:
- (a) Content that spreads false, misleading, or fake news, including disinformation and misinformation.
 - (b) Content that portrays nudity, pornography, adult materials, materials with sexual content, obscene images, or foul language.

- (c) Content that condones, promotes, contains, or links to warez, cracks, hacks, associated utilities, or other piracy-related information.
- (d) Content that promotes deviant teachings, extremist ideologies, or content that exploits, abuses, harasses, or endangers children or vulnerable individuals, including child sexual abuse material.
- (e) Content that has been promoted through unsolicited electronic communications (SPAM), mail fraud schemes, or pages that promote or condone the sending of unsolicited bulk email. Any bulk email originating from University servers or related to University web hosting accounts that is mass-distributed to any recipients for solicitation purposes may result in immediate account suspension.
- (f) Content that is grossly offensive to the community, including blatant expressions of bigotry, prejudice, racism, hatred, cyberbullying, cyberstalking, harassment, threats, intimidation, or online abuse, or content that is obscene, excessively violent, or otherwise objectionable.
- (g) Content that sells or promotes any unlawful products or services in the location where the content is posted or received.
- (h) Content that infringes or violates any copyright, patent, trademark, service mark, trade name, trade secret, or other intellectual property rights of any third party.
- (i) Content that promotes fraud, multi-level marketing (pyramid) schemes or other illegal or fraudulent activities.
- (j) Content that posts or discloses any personal data of, or private information about, any person without consent or authorisation of that particular person.

3.3.2 The above prohibition is not exhaustive and shall be read together with applicable Malaysian laws and regulations, including but not limited to the Communications and Multimedia Act 1998, Online Safety Act 2025, Penal Code, Cybercrimes Act 2026, Personal Data Protection Act 2010, Copyright Act 1987, Trademarks Act 2019, Cyber Security Act 2024 and any other relevant legislation and guidelines issued by the Malaysian competent authorities.

3.4 Data Handling and Protection

3.4.1. All University websites, web applications, and web hosting services must implement appropriate security controls, including the use of Secure Sockets Layer (SSL) certificates registered under the IIUM domain, to ensure data confidentiality, integrity, and protection.

3.4.2. All information collected must be handled, processed, stored, and protected in accordance with applicable privacy, personal data protection, and confidentiality principles, as well as relevant IIUM policies, guidelines, and applicable laws and regulations.

3.5 Software and Plugin Approval

ITD must approve any software or plugins before installation at IIUM websites, web applications and web hosting services. ITD reserved the right to reject any software or plugins that are deemed to pose security risks.

3.6 Financial Compliance

All websites, web applications and web hosting services that involve financial procedures, payments or financial transactions of any kind shall comply with the IIUM Financial Policies and Procedures.

3.7 Guidelines/Procedures

The implementation and adherence to this policy shall be carried out in accordance with the guidelines/procedures developed separately from this policy. These guidelines/procedures provide detailed steps, tools and actions required to ensure compliance with the policy's directions and objectives.

3.8 Compliance and Enforcement

- 3.8.1 The Director of the ITD holds the responsibility for the implementation of this policy and shall take necessary actions in the event of violation of this policy.
- 3.8.2 This policy is applicable to the University community, and any infringement of the policy may be subject to disciplinary actions and/or any other actions deemed necessary.

SECTION 4: ADMINISTRATION OF THE POLICY

4.1 Ownership of the Policy

The ITD is responsible for the formulation and maintenance of this policy.

4.2 Effective Date

This policy will take effect upon approval by the ICT Committee

4.3 Approval and Authority

The ICT Committee shall be the approving authority for this policy and matters related thereto.

4.4 Review and Revision Process

This policy shall be reviewed from time to time to ensure its continued relevance and effectiveness, with reviews conducted at least annually or as circumstances require.

4.5 Related Policies/Standards/Procedures/Guidelines

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

- 4.5.1 Communications and Multimedia Act 1998 (Act 588)
- 4.5.2 Online Safety Act 2025 (Act 866)
- 4.5.3 Penal Code (Act 574)
- 4.5.4 Cybercrimes Act 2026
- 4.5.5 Personal Data Protection Act 2010 (Act 709)
- 4.5.6 Copyright Act 1987 (Act 563)
- 4.5.7 Trademarks Act 2019 (Act 815)
- 4.5.8 Cyber Security Act 2024 (Act 854)
- 4.5.9 IIUM ICT Regulations
- 4.5.10 IIUM Financial Policies and Procedures
- 4.5.11 Policy on Procurement of ICT Resources
- 4.5.12 IIUM ICT Security Policy

- 4.5.13 Visual Identity (<https://www.iium.edu.my/office/ocap/corporate-identity-resources>)
- 4.5.14 IT Infrastructure Library (ITIL)
- 4.5.15 Control Objectives for Information and Related Technologies (COBIT)
- 4.5.16 IIUM Anti Bribery and Corruption Policy

Title of Policy	:	Policy on Website, Web Application and Web Hosting
Number of Policy	:	IIUM-ISMS-L1-013
Approving Authority	:	ICT Committee
Approval Date	:	24/09/26
Effective Date	:	24/09/26
Version No.	:	02
Revision No.	:	00