



Guideline on IIUM Website Development and Web Content- DRAFT

IIUM ICT GUIDELINES

PREPARED FOR:

International Islamic University Malaysia

PREPARED BY:

Information Technology Division

IIUM ICT Policy & Guideline

Document Change Log

Release Version	Date	Pages Affected	Remarks/Change Reference
Version 1.0	08/10/2024	All	Endorsement from ITD Management
Version 1.1	26/10/2025	4,7	

IIUM ICT Policy & Guideline

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Abu Hurairah A. Manaf	Endorsement from ITD Management	08/10/2024	10/10/2024
Abu Hurairah A. Manaf	Add clause 3.1, 3.2, 8.1.3	28/10/2025	

IIUM ICT Policy & Guideline

1. OBJECTIVE

The purpose of this document is to establish guidelines for the development of the IIUM website and its content.

2. TERMS AND DEFINITIONS

Term	Definition
IIUM	The International Islamic University Malaysia, otherwise known as the “University”
ICT	Information and Communication Technology
ITD	Information Technology Division
ITD Senior Management	Chief Digital Officer, Director, Deputy Information Technology Officer and Deputy Engineer of ITD
KCDIOM	Kulliyyah, Centre, Division, Institutes, Office and Mahallah
OCAP	Office for Communication, Advocacy and Promotion
CMS	Content Management System

3. GENERAL GUIDELINES

- 3.1 This guideline 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, recognizing 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.
- 3.2 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.
- 3.3 **Content Management System**
The recommended open-source content management system (CMS) is WordPress.
- 3.4 **Branding Compliance**

IIUM ICT Policy & Guideline

All branding elements, including the IIUM logo and corporate colours, must adhere to the Corporate Identity and Resources guidelines established by OCAP. For further details, please refer to the IIUM Visual Identity document.

3.5 Media Usage

Videos, images, and audio produced by IIUM must not be used for personal or commercial purposes.

3.6 Copyright Compliance

Avoid using copyrighted videos, images, or audio, as the university will not be held responsible for any legal issues that may arise from their use.

3.7 Credential Security

Do not share your login credentials or use the same credentials as those for personal accounts.

3.8 Password Management

Passwords must be reset every six months for security purposes.

3.9 Storage Approval

Approval from the IT Division (ITD) is required for any resource that requires substantial storage space, such as videos (maximum size: 1GB).

3.10 Payment Function Approval

The Finance Division must approve any payment-related functions or payment gateways.

4. SECURITY GUIDELINES ON WORDPRESS

4.1 Regularly Update WordPress Core, Themes, and Plugins

Ensure that the WordPress core, as well as all installed themes and plugins, are updated regularly to benefit from the latest security patches and improvements.

4.2 Implement Strong Password Policies

Use strong, unique passwords for all user accounts, including administrators, editors, and contributors. Consider employing a password manager to help generate and store complex passwords.

4.3 Limit User Permissions

IIUM ICT Policy & Guideline

Assign the minimum necessary user permissions for each role. Regularly review user accounts and remove any that are no longer needed to reduce the risk of unauthorised access.

4.4 Use HTTPS Encryption

Enable HTTPS by obtaining an SSL certificate for your site. This encrypts data transmitted between the user's browser and the server, enhancing security and improving search engine rankings.

4.5 Regularly Back Up Your Site

Schedule regular backups of your entire WordPress site, including the database and all files. Store backups securely and ensure they are easily accessible for restoration in case of data loss or security breaches.

4.6 Install a Web Application Firewall (WAF)

Implement a Web Application Firewall to filter and monitor HTTP traffic to and from your website. A WAF helps protect against various threats, including SQL injection, cross-site scripting (XSS), and other common vulnerabilities.

4.7 Monitor Site Activity

Regularly monitor your site for suspicious activity, such as unusual login attempts or changes to content. Consider using security plugins that provide activity logging and alert notifications for any anomalous behaviour.

4.8 Disable XML-RPC if Not Required

If XML-RPC functionality is not necessary for your site, consider disabling it to reduce the risk of brute-force attacks and other vulnerabilities associated with XML-RPC.

4.9 Use Security Plugins

Install reputable security plugins that provide features such as malware scanning, firewall protection, and login attempt monitoring. These plugins can enhance the overall security posture of your WordPress site.

4.10 Educate Users About Security Best Practices

Provide training and resources for all users with access to the site. Educate them on security best practices, such as recognising phishing attempts and maintaining strong passwords.

4.11 For detailed security practices, please refer to the official WordPress security guidelines available on their website

IIUM ICT Policy & Guideline

(<https://developer.wordpress.org/advanced-administration/security/>)

5. IMPLEMENTATION AND NON-COMPLIANCE

5.1 The Director of the Information Technology Division is responsible for the implementation of these guidelines and will take appropriate actions in the event of any violations.

5.2 These guidelines apply to the University community, and any infringement may result in disciplinary action and any other measures deemed necessary.

6. ENTITIES AFFECTED BY THIS GUIDELINES

All IIUM communities and KCDIOM entities that have and maintain formal websites.

7. MAINTENANCE OF GUIDELINES

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

8. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

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

- 8.1.1. ICT Regulations
- 8.1.2. IIUM ICT Policy
- 8.1.3. IIUM ICT Security Procedure
- 8.1.4. And any other related policies and guidelines