XIAMEN UNIVERSITY MALAYSIA
厦門大學馬來西亞分校

XMUM Website Hosting Service Policy

Objective

The XMUM website hosting service aims at providing a consolidated, fully monitored and secured website hosting service for University's faculties, departments, units and projects to publish and distribute information through setting up corresponding websites/homepages, so as to facilitate teaching and learning interactions, research activities and other educational purposes related to XMUM.

To apply for the XMUM Web Hosting Service, please fill in the **application form**. In order to protect the stability and security of the hosting service infrastructures and the websites resided in, the Website Service Hosting Policy has to be established as below.

1. Domain Name & Website Development

a) To provide better security and maximise the value of the University's investment in information technology infrastructures, all University related websites encouraged to be hosted on University Data Centre (On-Premise Hosting) and will ONLY be accessible via the **www.xmu.edu.my** subdomains.

b) Faculties, departments and units can apply for new university sub-domain name limited to following format (**www.xxxx.xmu.edu.my** or **www.xmu.edu.my/xxxx**).

c) The allocation of sub-domain names will usually be on a first-come-first-served basis. The IT Office may reject a name if it is considered inappropriate or if it may cause confusion about the purpose of a service it represents or conveys.

d) The inactive or unused domain names shall reallocate to another faculties, departments or units within the University community when it applies.

e) Applicants should make prior arrangement with the IT Office to get more information about the website hosting environment and to ensure conformance prior to website development. Otherwise, there will be no guarantee on the compatibility of development tools, software and the proper delivery of Website service.

f) Any website hosting via third-party developer/vendor should consult IT office to ensure the website implementation is adhered to the Universities website hosting and security standard policy.

g) To support accessibility, security and content management, all University's faculties and department websites, encouraged to be built on reliable Content Management System. (eg. WordPress, Drupal and etc)

h) In order to provide a stable environment for the website hosting service which already hosted, no development activities will be allowed in these hosting servers. Users are expected to do all developments and testing on their own machines before uploading to the XMUM web hosting servers.

i) Applicants or external third-party vendors only allowed to upload the final verified development files to the website hosting servers under the supervision of IT Office and strictly no private access to website hosting servers.

2. Website Administrator & Content Management

a) To assist with the management of website content, Heads of Faculties/Departments assign a permanent XMUM employee within the department to be the website administrator.

b) Website administrators are solely responsible for the security of their website administration credentials. Protect the website administrative login account information by using strong password combination and regular password change. Website administrator shall not pass the account information to other employee, students or unauthorised parties such as external developers. However, if it is unavoidable, website administrators are reminded to change their account passwords once the related party completed their task.

c) All the contents on the related websites should be reviewed each semester or at least annually.

d) Website administrators are solely responsible for the accuracy and the propriety of their website contents. They should also conform to the XMUM web hosting policy and the related University policies.

e) Website administrators are solely responsible to ensure:

- no materials that might cause anger or inconvenience to anyone/organization, or contrary to established policies in the campus and community.
- No advertising materials or materials relating to commercial and business activities.
- No harassing, defamatory, pornographic, obscene, indecent or distasteful contents

f) Ensure to provide contact details, or a link to contact information, for your Faculties, Departments, Schools and Unit, plus an email address for feedback to the website administrator.

g) Daily and Weekly system schedule backup of website hosting servers will be performed for service recovery purposes. However, website administrators are advised to maintain a copy of their own (both application and data).

3. Security & Upgrades

a) The website will be subject to periodic vulnerability scans for protection against known or potential information security threats, and site administrators will be notified if any changes or updates are required.

b) The IT Office will timely apply official security patches released by the Operating System or Hosting Software vendors. Although the patches normally will not affect website hosted in the hosting servers, however, should this occur, it will be the responsibilities of the website administrator seek initial website developer/third-party vendor to resolve the problem. To protect the hosting server and the other website hosted, security patches applied will normally not be removed even though they cause problem with some website or applications.

c) The website Developers/Programmers should have operational awareness of security concerns to prevent any vulnerabilities and security threat on University's websites including:

- maintenance of appropriate access control on files and directories
- maintenance of appropriate access control on resources such as databases
- the potential for cross-site scripting and cross-site request forgery
- the potential for session fixation and hijacking
- the potential for SQL injection

- the need for appropriate encryption during secure transactions and data storage, and
- the appropriate use of existing authentication frameworks.

d) If website is found to be causing problems or presenting a security threat, or enabling illegal activity, the website administrators will be notified and expected to take corrective action immediately.

e) The university websites are open to public access, therefore content stored should be properly protected and encrypted. Under no condition should it be used for store sensitive data. SSL certificate is required to protect sensitive information

f) IT Office does not provision SSL certificates and website administrator can apply and purchase SSL certificate from trusted CA (certificate authority).

Copyrights and Violations

a) The University respects copyrights and other intellectual property rights and will do its best to comply with the applicable copyright laws, regulations and guidelines. The University is concerned with possible infringement of copyright and other intellectual property rights by its staffs and students, and for which the University may have vicarious liability. All Faculties/Departments/Units are therefore requested to help ensure compliance with the applicable laws, regulations and guidelines, and suggest precautionary measures.

b) Website administrator must ensure:
   - Obtain permission from copyright owner concerned prior to publishing any material.
   - Be aware that rights for web publication is not equivalent to rights for print publication, and need to be negotiated separately.
   - Ensure appropriate credits for materials used.

Service Rights and Termination

a) Should the websites hosted in the XMUM hosting servers become the target of a network attack or a target of the investigation arisen from a security incident, the IT Office

reserves the right to take any necessary actions in order to restore normal operation including:

- Restrict the access to the website
- Disable dangerous files by moving or deleting them
- Terminate processes
- Disable the web site from access
- Remove the website administrator's access to the site (e.g. if compromise is suspected)

b) The IT Office may, without prior notice, terminate a faculties, departments or units hosted website services, if such service violates of the XMUM web hosting policy or other related University policies. IT Office will not be liable for any damages or loss resulted from such termination.

Administrator Acknowledgement	Supervisor Acknowledgement
Signature Name: Date:	Signature Name: Date: