Server Hosting Policies on the University of Lagos Network (ULN).

The University of Lagos website (ULW) provides links to and information about the University, its teaching and research mission, its academic programmes, resources, services and people, to a wide audience of staff, students, alumni, faculties, collaborators, potential employers and visitors. Therefore it is important that the web pages provide the best possible representation of University of Lagos.

The University of Lagos Server Hosting Policies (ULSHPs) outlines the principles and conventions that provide the foundation for developing and publishing University of Lagos websites. It is intended to govern the University's web presence as it relates to reputation, risk, security, hosting practices and naming conventions. It applies to all websites representing the University, regardless of where they are hosted.

With a view to providing a reference site for all departments and offices to refer to when they engage in web publication, the Centre for Information Technology and Systems (CITS) has prepared this guide to the related policies, design guidelines, references etc. that are relevant and certainly useful for publishing and hosting of servers on the University of Lagos Network (ULN).

Policy

Policies governing naming convention

Maintaining a strong and consistent visual identity for the University helps increase recognition, respect and awareness and projects the University's reputation for excellence in education. One element of recognition that supports the University's identity is the naming convention on University websites. To support a consistent identity on the web, the following web naming principles and conventions apply:

i. www.unilag.edu.ng normally will be used for all official University websites and sub-sites and will follow a nested naming structure.

ii. Subdomain.unilag.edu.ng will be used for web applications

Policies governing web publications

While the Networking and the Web teams of CITS are responsible for the physical maintenance of servers hosted at the University of Lagos Data Centre, Web publishers at the University of Lagos are responsible for the contents of the pages they publish and are expected to abide by the highest standards of quality and responsibility. These responsibilities apply to all publishers, from academic departments to administrative offices. In addition, publishers should make sure that the use of resources is tied firmly to the mission of the University of Lagos and all web activities must support research, education, administrative processes, community service and legitimate pursuits. They are also required to comply with relevant University of Lagos rules and policies, and international and local laws concerning appropriate use of computers, information and data security.

Policies governing web hosting environment

Because of physical security and routing nature of the University of Lagos Network (ULN), all servers and websites are to be hosted at the University of Lagos Data Centre (ULDC). It is therefore the responsibility of both the Network team, the Web team and the Web publishers to perform proper server management to ensure the server is secured from hacking and attacking activities. Below are some guidelines and notes for maintaining servers hosted on the University of Lagos

Network.

a. All servers must be rack mountable;

b. All servers must be standard supportable hardware;

c. All hosted servers must undergo a security conducted by the CITS personnel and data center teams;

d. All servers must have redundant power supplies;

e. Apply a domain name for the web server and avoid using IP address in the URL;

f. Devise a backup strategy for backing up the website information and data;

g. Apply latest OS patches;

h. Turn on Firewall (if any) to protect the server;

I. Install **only** anti-virus program authorised by the University of Lagos and apply its latest patch. Set schedule to update or download the latest virus definition file;

j. If it is a Windows server, install Microsoft Baseline Security Analyzer and run it regularly.

Consequences for Noncompliance

If risks are not mitigated, the University’s reputation could be harmed. Websites representing the University could contain inaccurate, misleading, libelous or illegal content, and student or financial information (e.g. credit card numbers) could be at risk. If privacy laws are not complied with (particularly for websites hosted on servers in other countries) the University may be legally liable. Failure to comply with the above policies may result in removal of content, disabling of the website, or disciplinary action as follows:

a. In cases of externally hosted websites, requests for immediate compliance will be sent to site owner;

b. Websites hosted on the University’s web infrastructure may be subject to immediate action without notice. Site owners who fail to secure and/or maintain these sites will be given 30 days to comply, after which the site will be disabled.