Security Guidelines for Building Websites or Web Applications for Project Owners and Vendors

It is necessary to observe and check with the following areas when a website or web application project is started.

Roles of Project Owners and Technical Owners

- Every project needs to have a project owner to oversee the overall management of the project.

- Besides defining all the requirements of the project, a project owner also needs to appoint a technical owner (or a vendor if the project is outsourced) to check with all technical requirements of hosting services and IT security policies.

- Project owners and technical owners need to review the Cybersecurity Policy (https://itsc.ust.hk/it-policies-guidelines/cyber-security-policy-executive-summary/) and ensure their websites and web applications fulfil the requirements wherever appropriate, specifically

    o Risk Assessment, Classification and Mitigation - https://itsc.ust.hk/it-policies-guidelines/risk-assessment-classification-and-mitigation/

    o Minimum Security Standard, Acceptable and Recommended Practices - https://itsc.ust.hk/it-policies-guidelines/minimum-security-standard-acceptable-and-recommended-practices/

    o For systems containing sensitive data, the corresponding departments shall consult ISO to explore the appropriate technical option.

Vulnerability Scanning for Websites and Web Applications

- Technical owners need to ensure their websites or applications are free of any high-risk security vulnerabilities. All high-risk security vulnerabilities should be resolved before the launch of a website or web application.

- More information about Service of Web Application Health-check Scanning - http://itsc.ust.hk/services/cyber-security/web-application-health-check-scanning

ITSC Web Hosting Solution Overview

The following hosting options are available for hosting websites or web applications. Please also refer to the Terms and Conditions and Usage Policies of various hosting solutions.

	iHost 2.0	Virtual Server (VaaS)
Overview	iHost allows users to build their own websites with database queries in a secure web hosting environment with common website configurations.	Users have full control of rented virtual servers which run on either Windows or Linux[2] and are free to install software tools and build programs to fulfil their own needs.
Feature Highlights	• Support PHP and MySQL with Apache on Linux [1] • High flexibility to host common website contents and customize website settings • Different from the old iHost, iHost 2.0 allows to run PHP files outside "cgi-bin" folder	• Full flexibility to host any website contents and programs supported in the selected Windows or Linux [2] • Server capacity can be purchased and extended
Best used for	• Specific requirements for website contents and features	• Complex websites with specific requirements and custom-made solutions • Dedicated server capacity and performance are required
Technical Expertise Required	Medium to High	High
Maintenance & Responsibilities (ITSC)	• ITSC regularly apply security patches to maintain the security level of the hosting environment	• Nil
Maintenance & Responsibilities (Users)	• Websites need to comply with Cybersecurity Policy and Application Minimum Security Standard • Website owners need to dedicate technical staff (or vendors) as Technical Owners for website maintenance such as resolving security vulnerabilities in the lifespan of the websites	• Servers and websites need to comply with Cybersecurity Policy, Application Minimum Security Standard and Server Minimum Security Standard • Website owners need to dedicate technical staff (or vendors) as Technical Owners for both website and server maintenance such as resolving application vulnerabilities and system patching in the lifespan of the websites.
Data Security	Storing of high risk data **NOT** allowed	Storing of high risk data allowed
Hosting Fee	Free	VaaS Pricing
More Information	iHost 2.0	VaaS Hosting

---

[1] iHost 2.0 currently supports PHP 5.5.9, MySQL 5.5.52, Ubuntu 14.04.1

[2] Supported Operating Systems are Windows Server 2008 R2, Windows Server 2012 R2, CentOS 6 / 7 64-bit edition, Ubuntu Server 12.04 LTS / 14.04 LTS 64-bit edition