1.0 PURPOSE

The purpose of this document is to provide a clear understanding on the management of Responsibility Centres's (RC's) websites that are being put in the web hosting server(s) of Department of Information Technology (JTM) based on the risks identified and international best practices.

2.0 SCOPE

The scope of this document covers all websites in the web hosting servers under the management of JTM.

However, the scope of the Information Security Management System (ISMS) audit and certification only covers JTM's staff and JTM's assets that are located in the JTM premises.

3.0 BEST PRACTISE

3.1. Responsibilities of RCs

3.1.1. Only official websites from the following departments can be hosted by JTM:

(i)   Responsibility Centres
(ii)   Associations
(iii)   Uniform bodies recognized by UM
(iv)   Research Centres
(v)   Residential Colleges

Others may be considered, if approved by the JTM management

The Responsibility Centres, Associations, Uniform bodies, Research Centres and Residential Colleges will be referred to as RC in this document.

3.1.2. Only websites that have been scanned and confirmed without vulnerabilities will be allowed to use the web hosting services.

3.1.3. Websites placed in the web hosting servers must comply to the environment listed below:

3.1.4. RC has to apply at least 3 weeks before placing their websites in the web hosting server in JTM. During this period, the websites will be scanned for vulnerabilities.

3.1.5. RC is fully responsible for the contents of the website placed in the web hosting server.

3.1.6. RC has to practice secure coding to ensure the security of the website.

3.1.7. RC has to ensure only official sites are operating in the website.

3.1.8. RC is to send an official letter to JTM requesting the website to be closed when the web hosting services are no longer required.

3.1.9. RC has to cooperate with JTM to recover data and services should the website experience problems or is corrupted.

3.1.10. RC has to appoint a certified webmaster to manage the website as well as the security aspects of the website.

3.1.11. RC is responsible to safeguard the password given by JTM.

3.1.12. RC is responsible to do backup for the hosted website.

3.1.13. RC has to monitor the version of the programming language, the content management system engine, plugins, or any related tools (if applicable) and upgrade them if any security issues exist. JTM has the rights to close the website if no action was taken to address the vulnerabilities within a month.

3.1.14. If there is any security issue on web hosting application, RC will be responsible to ensure they are resolved.

3.1.15. RC is fully responsible for the development and maintenance process of their website.

3.2. Responsibilities of RCs

3.2.1. Liaise with RC's representative on matters concerning JTM's web hosting services and facilities.

3.2.2. Ensure backup for the website is being implemented according to the details stated in RC's application form (Commercial Web Hosting Services Only, based on SLA).

3.2.3. Ensure the security of the web hosting servers by doing the necessary updates and patching, as well as monitoring web hosting server security, on a continuous and periodic basis.

3.2.4. Ensure the webserver and database of the website are continuously available. If there are any problems, implement the workaround to revive the website according to the procedure given by the RC. If unsuccessful, communicate with RC.