Service Improvement Details & Recommendations

S. No	Activity Description	Remarks
1	It would not be recommended to give Administrator privileges for client users in shared server.	To enhance Security
2	It would be recommended to update timely patches on the client PC OS who are accessing Server via VPN. (According to the latest Policy of Microsoft to access the server via RDP, both the client and server should be updated with the latest patches).	To enhance Security
3	The vendor shall get the security audited by third party expert periodically (once in six months) to ensure and guarantee security of the data center	To enhance Security
4	It is recommended not to reveal passwords on mails. Since it is observed that the end client/vendors are forwarding the mails which contains all the credentials of VPN as well as server for the further service requests. We recommend User id and credential to be delivered only to the concern nodal officer's (in official mail id only – one to one) mentioned in the request form.	To enhance Security
5	Antivirus software protects systems from virus infection. It is recommended software is Properly configured and updated. Antivirus software need to be implemented on all systems connected in network.	Need to procure Antivirus Software license
6	It is highly recommended Only licensed and authentic versions of software need to be used by all the stakeholders.	Need to procure license for concerned Software
7	For critical applications, a disaster recovery with online replication needs to be maintained. A continuous standby needs to be maintained for the application such that recovery is immediate and downtime is minimum.	In order to maintain data redundancy
8	Recommended to Use SSL Certificate Site wide on all websites & applications. The SSL Certificate should use at least 2048-bit SHA 256 encryption or higher. Ensure that the SSL Certificate is valid and keep track of the certificate expiry date and take necessary action to renew/replace the certificate before expiry. Disable support for SSL 2.0, SSL3.0, TLS 1.0 at the server level. Use TLS 1.2	Need to procure SSL certificate
9	Preventing direct root login to virtual console devices helps ensure accountability for actions taken on the system using the root account.	To enhance Security

10	Back up website files regularly.	To enhance Data Security
11	It is recommended to update timely IOS/Firmware on the Network devices.	To enhance security
12	It is recommended to update timely licenses for Network Security devices.	To enhance security updation and new features.
13	Log analysis is recommended on a daily basis and an action plan prepared based on the findings.	To enhance security
14	We would not recommend allowing network ports like Telnet-23, RDP-3389, MS-SQL-1433, Mysql3306 etc. or ports that directly connects to our device, server, database, internal access or public internet and VPN service.	To enhance security
15	The vendor shall get the security audited by third party expert periodically (once in six months) to ensure and guarantee security of the data center	To enhance security
16	It is recommended the websites are mainly run on standard port, https/443 , http/80 and some other nonstandard port as http/8080, http/8082, https/8443, https/9443	To enhance security
17	It is recommended to disable internet service on physical and virtual servers.	To enhance security
18	It is highly recommended not to white list public IPs which were once already black listed	To enhance security
19	It is highly recommended not to allow unwanted url/website/application (Social media, news etc.)	To enhance security
20	We recommend VPN profile validity should not exceed 45 days.	To enhance security
21	Recommended to allow VPN profile only on staging servers and not on production servers.	If VPN connectivity on production server is required, VPN undertaking letter needs to be submitted to DCO
22	It is recommend to upgrade from Wampserver 2.5 to Wampserver 3.0.3	To enhance security and performance
23	Logins need to expire after a short period of inactivity at application level.	Recommended Idle time 30 minutes
24	Strong passwords need to be used and NEVER be written down.	To enhance security. Never to use dictionary words, name, pet names and DOB
25	All devices plugged into the network need to be scanned for malware each time they are plugged in.	To enhance security
26	All site content updation shall be done only by the site owner over VPN or by visiting Goa SDC and updating in presence of DBA Team.	To enhance security

27	Site configuration files must be secured. (php.ini configurations etc.)	To enhance security
28	Site shall be configured such that any file uploaded in the file upload folder system area, using the CMS file upload functionality, is not able to run as an executable file. The file upload folder area in the system should have read and write permissions only.	To enhance security
29	Sites built with the CMS module must be audited mandatorily. Any downloaded components such as PHP-nuke, Asp based codes must also be audited.	To enhance security
30	Database admin components such as PHPMyadmin on the host server must either be limited to restricted access to console or removed. It is seen that this is often used as a vector to attack in PHP based sites.	To enhance security
31	The CMS link (and folder) should preferably not be named as “admin” or “control” etc, which can be guessed easily.	To enhance security
32	The CMS should be hosted on SSL for the CMS virtual directory, with SSL-certificate based authentication.	To enhance security
33	Write permission should not be given to User running Webserver service on root folder and subfolders.	To enhance security
34	All the websites plugins and themes of CMS should be validated by vendor.	To enhance security
35	The production site should have gone through complete security audit process. Verify that all audit recommendations are applied on the production site and the code hardened accordingly.	To enhance security
36	It is highly recommended to restrict directory listing i.e. Source code should not be visible in internet world.	To enhance security
37	Any change in the source code of the audited web application requires to undergo a Vulnerability Assessment / penetration testing	To enhance security
38	Credentials used during testing should be mandatorily changed in production server.	To enhance security
39	The Site Owner (Content Manager) of each site is responsible for the updating and maintenance of content for the site. He/she 1. Shall have VPN access to the server, with authentication. 2. Shall update contents only over VPN. 3. Shall be provided with privileges to read/write/create folder, delete folder, and directory traverse in the website’s document root folder.	To enhance security
40	Recommended to take Back up website files, configuration files and databases on regular basis	To enhance Data Security
41	Recommended to set Strong Passwords using alpha-numeric and special Characters.	To enhance security

42	Recommended to Remove Anonymous Users.	To enhance security
43	Highly recommended to Remove test database.	As per standard policy
44	Recommended to Remove and disable the database history file.	As per standard policy
45	The application should connect with the database using a low privileged database user having minimum required database privileges.	To enhance security
46	Keep CMS Core, Themes, and Plugins Up to Date	To enhance the security of websites
47	Only Install Trusted CMS Plugins and Themes	To enhance the security of websites
48	Remove Unused Plugins and Themes	To enhance the security of websites
49	Install a Security Plugin 1.Sucuri Security2.Ithemes Security3.Bulletproof Security	To enhance the security of websites
50	Limit Login Attempts to Admin panel or any Login pages	To enhance the security of websites
51	Monitor Incoming Attacks	To enhance the security of websites
52	Hide Your CMS Version	To enhance the security of websites
53	Relocate or Rename Login Page	To enhance the security of websites
54	Secure the Wp-config File	To enhance the security of websites