CH 08 Website Hosting

Website Hosting

8.1 Website Hosting

The fundamental purpose of a Government website is to deliver the information and services to the citizens and other stakeholders using the medium of Internet. Generally, websites/portals/web applications are hosted on special purpose servers in a Data Centre.

Data Centre is a facility equipped with controlled power, cooling, systems, physical security and access control. Generally, a large number of servers are hosted in a Data Centre, powered by high speed networking infrastructure, storage system along with a storage network. Provision for back-ups of data/information residing in Data Centres is also an important service of Data Centre. Multi-tier security infrastructure is also a crucial component of Data Centres.

While it is extremely important to develop websites using state-of-the-art technologies, hosting infrastructure plays a crucial role in the performance, availability and accessibility of these websites to end users with varying set-ups.

Hence, configuration of hosting server infrastructure as well as facilities at Data Centres is an important aspect to review, prior to hosting. Following section details the kinds of facilities and services that the Department should expect from their hosting service providers.

8.2 Hosting Service Provider

8.2.1 Indian Government websites MUST be accessible to the public in a fast and secure manner on 24x7 basis. It is important that the Web Hosting Service Provider (HSP) for a government department be chosen with extreme caution and care and the following have to be kept in mind :

a. The HSP MUST possess state-of-art multitier security infrastructure both at physical and network level as well as security policies to ensure the best possible security to Government websites.

b. The Web Hosting Service Provider MUST also use devices such as firewall and intrusion prevention systems to make the website more secure.

c. The Web Hosting Service Provider MUST have a redundant server infrastructure to ensure fastest restoration of the website in the event of any unforeseen hardware/software failure.

d. The HSP MUST perform regular backups of the websites. It is also advisable to conduct a mock test of restoration of data once in a while to plug any loopholes.

e. The HSP MUST have a Disaster Recovery (DR) Centre in a geographically distant location and a well drafted DR plan for fast restoration of the services during any disaster.

f. Provision should be given to the concerned Department to remotely update their website in a secured manner.

g. The HSP should also provide the facility of staging infrastructure in order to facilitate the testing of the new websites as well as their enhanced or revised versions content prior to publishing on the internet.

h. HSP should provide web server statistics required for performance evaluation on a regular basis. If possible, online access to the traffic analysis should be provided so that the Department can access the traffic analysis at any point of time for the purpose of evaluation.

i. Web Hosting Service Provider MUST provide helpdesk & technical support to the department on 24 x 7 x 365 basis.

8.3 Contingency Management

The website of a Government Department is its presence on the Internet and it is very important that the site is fully functional at all times. It is expected of the Government websites to deliver information and services on a 24x7 basis. Hence, all efforts should be made to minimise the downtime of the website as far as possible.

It is therefore necessary that a proper Contingency Plan MUST be prepared in advance to handle any eventualities and restore the site in the shortest possible time. The possible contingencies include:

8.3.1 **Defacement of the website:** All possible security measures MUST be taken for a Government website to prevent any possible defacement/hacking by unscrupulous elements. However, if despite the security measures in place, such an eventuality occurs, there must be a proper contingency plan, which should immediately come into force. If it has been established beyond doubt that the website has been defaced, the site must be immediately blocked. The contingency plan must clearly indicate as to who is the person authorised to decide on the further course of action in such eventualities. The complete contact details of this authorised person must be available at all times with the web management team. Efforts should be made to restore the original site in the shortest possible time. At the same time, regular security reviews and checks should be conducted in order to plug any loopholes in the security.

8.3.2 **Data Corruption:** A proper mechanism has to be worked out by the concerned Government Departments, in consultation with their web hosting service provider to ensure that appropriate and regular back-ups of the website data are being taken. These enable a fast recovery and uninterrupted availability of the information to the citizens in view of any data corruption.

8.3.3 **Hardware/Software Crash:** Though such an occurrence is a rarity, still in case the server on which the website is being hosted crashes due to some unforeseen reason, the web hosting service provider must have enough redundant infrastructure available to restore the website at the earliest.

8.3.4 **Natural Disasters:** There could be circumstances whereby due to some natural calamity, the entire data center where the website is being hosted gets destroyed or ceases to exist. A well planned contingency mechanism has to be in place for such eventualities whereby it should be ensured that the Hosting Service Provider has a 'Disaster Recovery Centre (DRC)' set up at a geographically remote location and the website is switched over to the DRC with minimum delay and restored on the Net.

Apart from the above, in the event of any National Crisis or unforeseen calamity, Government websites are looked upon as a reliable and fast source of information to the public. A well defined contingency plan for all such eventualities MUST be in place within all Departments/organisations so that the emergency information/contact help-lines could be displayed on the website without any delay. For this, the concerned person in the Department responsible for publishing such emergency information MUST be identified and his/her complete contact details should be available at all times.