BEML WEBSITE POLICY

CONTINGENCY MANAGEMENT

The presence of the website on the Internet and very importantly the site is fully functional all the times. It is expected of the Government websites to deliver information and services on a 24X7 basis. Hence, all efforts should be made to minimize the downtime of the website as far as possible.

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

- **Defacement of the website:** All possible security measures must be taken for the 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.
- **Data Corruption:** A proper mechanism has to be worked out by the concerned 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.
- **Hardware/Software Crash:** Though such an occurrence is a rarely, 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.

- **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 is should be ensured that the Hosting Service Provider has a 'Disaster Recover 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 al such eventualities must be in place 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 the complete contact details should be available at all times.