

## Contingency Plan

### **Contingency Management Plan**

The website reflects the efforts of Ministry of Road Transport and Highways in bringing citizen centric services of our country's transport sector online. There are more than 300 services offered and more than 100 of them are completely online. It is very important the website is always fully functional. It is expected that the Ministry will deliver services and information at 24x7 basis. Therefore, efforts have been taken to ensure minimal downtime as well as implementation of a Contingency Management Plan to ensure recovery of the website in minimum time possible after any eventualities. The possible contingencies have been highlighted below

1. Defacement of the website – All possible security measures must be taken by NIC (National Informatics Centre) to prevent any defacement/hacking by any foreign elements. However, in case of any happening despite the security measures, the contingency plan must immediately be able to put into force. If it has been established that there is a defacement, then the website must be immediately blocked. The contingency plan must clearly indicate as which authorized office will be decision making body do decide on further course of action at the earliest. At the same time, regular audits and checks must be ensured to gauge any loopholes that arise during the regular course of website operation
2. Data Corruption –A proper mechanism is followed by NIC in consultation with the web hosting service provider to ensure that regular back-up of website content is taken to enable swift recovery and availability of information to the citizens throughout.
3. Hardware/ Software Crash – In spite of the rarity in occurrence of this event, the web hosting provider must have enough backup hardware to reinstate the website at the earliest hour to facilitate smooth execution of citizen services
4. Natural Disasters – In unforeseen circumstances, there is a bleak possibility that the entire data centre withholding the information of website and related data is annihilated. A well planned contingency management needs to be in place to mitigate the risk associated with such eventualities. Mostly, the web hosting service provider is required to maintain a “Disaster Recovery Centre” in a geographically remote location and the website is usually routed to the DRC with minimal delay and restored to provide service to the citizens

[View PDF](#)