CONTIGENCY MANAGEMENT POLICY

(i) Defacement of the website: All possible security measures must be taken for the Bank 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 be executed. If it has been established beyond doubt that the website has been defaced, the site must be immediately brought down. The contingency plan must clearly indicate as who is the person authorized to decide on the further course of action in such eventualities. The complete contact details of this authorized person must be available at all times with the web communication team. In case of any defacement and data corruption, quick action needs to be taken by the respective authorized personnel for the same. 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 gaps in the security.

(ii) Data Corruption: A proper mechanism has to be worked out by the concerned Wing/Section, in consultation with their web hosting service provider, to ensure 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.

(iii) 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.

(iv) Natural Disasters: There could be circumstances wherein 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 wherein 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 Web.

In case of any Cyber security incident (Including Website defacement/Data leakage/data corruption…etc.), the same is to be reported to ciso@canrabank.com/ hoisg@canrabank.com immediately upon identification.