

Contingency Management Plan

1.1 Contingency Plan in the event of defacement

A.1.1. Defacement Protection Policy

- The **CEA website** undergoes regular security audits to identify and mitigate application vulnerabilities while ensuring optimal performance and compliance with cybersecurity standards.
- Any modifications at the application level necessitate a security re-audit to maintain the integrity and resilience of the system.
- All the servers' configuration and logs are monitored and timely action taken by NIC.
- Access to servers is strictly restricted to authorized system administrators by NIC
- All servers are secured and maintained by NIC.
- Content updates are conducted exclusively via secure FTP over a VPN, ensuring data confidentiality and integrity during transmission.

A.1.2. Monitoring of defacement of CEA website

To ensure the integrity and security of the CEA website continuous monitoring is done through the following mechanisms:

1. NIC actively monitors the website by analyzing log files for any unauthorized modifications or security threats. NIC Data Centre also conducts periodic assessments to detect any signs of defacement or undesirable changes.
2. The Development Team routinely inspects the website for anomalies or unauthorized modifications. In case of any security breach or defacement, the issue must immediately be notified to the Technical Manager and Web Information Manager via phone and email for prompt action.

A.1.3. Actions to be taken after defacement

In the event of a website defacement, the following steps will be taken to mitigate the impact and restore normal operations:

- Depending on the severity of the defacement, the website may be temporarily taken down or partially restricted to prevent further damage.
- Security teams will analyze log files to identify the source of the defacement and take necessary actions, including blocking malicious access.
- The type and extent of the defacement will be assessed, and necessary corrective measures will be implemented.
- In case of complete data loss, website data will be restored from the latest backup.
- Identified vulnerabilities will be patched based on security recommendations.
- A re-audit of the application will be conducted to ensure compliance with security best practices.
- Any affected or corrupted content will be restored from backups to ensure website integrity.

A.1.4. Contact details in case of any eventuality of defacement

Name	Designation	Organization	E-mail Address	Telephone/Mobile No.	Office Address
Surabhi Agrawal	Assistant Director	Central Electricity Authority	surabhiagrawal.c ea@gov.in	011-26732436	3 rd Floor, IT Cell & Procurement Division, Central Electricity Authority, Sewa Bhawan, R K Puram Sector – I, New Delhi-110066
S Mahalingam	Scientist F	National Informatics Centre	mahalingam@go v.in	9891123108	Ministry of Power, Shram Shakti Bhawan, Rafi Marg, Sansad Marg Area, New Delhi, Delhi 110001

A.1.5. Time for Restoration of the CEA website after defacement

The time required to restore the CEA Website depends on the extent of the defacement and the services impacted. A decision will be taken to restore in consultation with NIC as per their suggestion.

1.2 Data Corruption

To ensure uninterrupted availability and rapid recovery in case of data corruption or system failure, regular backups of website data are securely maintained at the NIC Data Centre. IT Division of CEA also takes regular backup of database for faster recovery.

1.3 Hardware/Software Crash

While server failures are rare, contingency measures are in place to ensure rapid recovery in the event of a crash. The NIC Data Centre, as the web hosting service provider, maintains a redundant infrastructure to restore the website with minimal disruption.

In such cases, the estimated time required to migrate and restart the website on an alternate server is approximately 24 hours to 48 hours.

1.4 Natural Disasters:

- In the event of a natural calamity or catastrophic failure that impacts the primary data centre hosting the CEA (Central Electricity Authority) website, an alternate site plan is in place. NIC would provide VM at an alternate site for restoration of

CEA website. This would typically involve switching DNS records or redirecting traffic to the alternate VM site, ensuring minimal downtime for end-users.

- The NIC team would monitor the transition and make sure that the alternate VM site is fully operational and capable of handling the website traffic, providing necessary support as required.
- NIC must ensure that transition to the alternate VM site would be seamless, minimizing downtime for users accessing the CEA website.
- During any such event, NIC/ CEA should notify users about any potential disruptions in service, or inform them once the website is fully restored.

