CODEC Networks Private Limited
Head Office: 507, New Delhi House, Barakhamba Road, New Delhi 110001
Contact No.: +91 11 43752299, 9971676124
Email: projects@codecnetworks.com
Web: www.codecnetworks.com

Decoding Threats, Coding Solutions

Safe to Host Certificate

Dated: 14th January 2025 **Cert No.:** CNPL24-25100125446

Client Name:	Centre for Development of Telematics (C-DOT)
Client Address:	C-DOT Campus, Electronic City Phase 1, Bengaluru – 560100
Application Name:	Mandatory Testing & Certification of Telecom Equipment (MTCTE) Portal
Purpose of Application:	A portal being used by Telecommunication Engineering Centre (TEC) to grant online certification to all telecom equipment that meets all TEC-prescribed Requirements.
Application Version:	4.0
Hosting URL:	https://mtcte.tec.gov.in/
Testing URL:	https://msso.cdot.in/
Audit Methodology:	OWASP Top 10 & OWASP Web Security Testing Guide (WSTG)
Tool Used:	Nessus Professional, Burpsuite Professional, Nmap & NSE, OSINT Tools, Manual Test Methodologies, Exploit DB Database
Current Version Hash:	d46ebe9dd9271f2627dcf9c6c0a33eff
Hash Algorithm:	MD5SUM
Testing Dates:	27th November 2024 till 10th January 2025
Name of Audit Company:	Codec Networks Private Limited
Audit Team Members:	Mr. Gaurav Pant, Mr. Himanshu Chauhan
Reviewed By:	Mr. Piyush Mittal, Head – Projects (Email: piyush@codecnetworks.com)

To Whomsoever It May Concern

This to certify that the tested application hosted of the current version has been tested for security vulnerabilities by Codec Networks Private Limited (A CERT-In Empaneled Organization wide letter No: 3(15)2004 CERT-In (Vol.XI) dated 12.02.2021) and it has been fixed by the client for OWASP vulnerabilities and any known severe web vulnerability/threat. Respectively the application revalidation test was carried out and the web application has passed Critical / High / Medium vulnerabilities for application security assessment tests.

For detailed description of vulnerabilities and other security assessment related details, please refer to the audit report shared with respective client.

It is also recommended that the application may be hosted with read and script execution permission for public with exact replica of the audited URL in the production environment.

Certificate Validity: The maximum validity of the certificate is One Year from the date of issue.

Note: Our opinion is valid for the period during which the changes are not made in the source of tested application thus any changes in the system will require to re-audit of application's new version. Projections of any conclusions based on our current findings will not be applicable and has to be altered for future period and application new versions is subject to any risks because of changes made to the application or system. Also, we recommend that Web Server and OS level hardening need to be in place for the production server.

Thanks & Regards,

Piyush Mittal
Project Manager; Codec Networks Private Limited