

DR CBS CYBER SECURITY SERVICES LLP

LLP Id No. AAK-4058

CERT-In Empanelled Information Security Auditing Organization (2020-2027)
Certified **ISO 9001:2015** (No. IN/24614556/4628), **ISO/IEC 27001:2022** (No. IN/26314557/3260)

Registered with **MSME** No.: UDYAM-RJ-17-0052608 &

Government e-Marketplace **GeM** Seller Id: IZ8O210002192567

Certificate of Recognition as **#Startupindia** No.: DIPP77174

Registered with iSTART **Startup Rajasthan** No.: 5F7054D

Member Data Security Council of India (**DSCI**): DSCI/AM/2018/03

Thursday, 6th March 2025

Safe To Host Certificate

Certificate Number	: 468/24-25/1324
Organization Name	: Consulate General of India, Shanghai
Address	: Consulate General Of India,10 Floor,1008, Shanghai International Trade Centre,2201, Yan An (West) Road, Shanghai-200 336 (P.R. China)
Application Name	: Consulate General of India, Shanghai
Testing/ Staging URL	: https://audit.cgishanghai.gov.in/
Production URL	: https://cgishanghai.gov.in/
Audit Period	: 10 th February to 6 th March 2025
Compliance Verification Date	: 6 th March 2025
Hash Value	: 63B52A920CB1034A32C07E2E228E0D38
Path	: /home/audit/public_html
Certificate Validity	: 1 year (Valid till 05.03.2026)

The above web application has undergone through IT (Cyber) Security Audit by our organization through provided Test URL as per guidelines, advisories, white papers and vulnerability notes issued by Indian Computer Emergency Response Team (CERT-In). We also tested the web application against various Web Security Standards like Open Web Application Security Project (OWASP) Comprehensive Framework, Directions by CERT-In under Section 70B, Information Technology Act 2000, Guidelines for Secure Application Design, Development, Implementation & Operations, SANS Top 25 Software Errors, Common Weakness Enumeration (CWE), Common Vulnerabilities and Exposures (CVE), The Web Application Security Consortium (WASC) and Web Content Accessibility Guidelines (WCAG) etc.

The audit was conducted on the given staging environment, not in production environment.

Conclusion: The application is free from any known vulnerabilities as on date.

The Certificate shall be deemed invalid if the underlying IT infrastructure of the web application gets modified after compliance audit.

Other Recommendations:

1. Web Server Security and the OS hardening need to be in place for the production server, it is also recommended to deploy and proper configure the SSL.
2. Web Application should comply with Guidelines for Indian Government Websites (GIGW).
3. Organization must comply with the Directions issued by CERT-In dated 28 April 2022 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.
4. The Developer Team must follow the Technical Guidelines on Software Bill Of Materials (SBOM) issued by CERT-In dated 03.10.2024.

Prepared By
DRCBS-24-037



Dr C B Sharma IPS (R)
Certified Lead Auditor ISMS ISO/IEC 27001:2013
Founder & CEO