



# 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)**

**Certified ISO/IEC 27001:2022 (No. IN/26314557/3260)**

**Thursday, 31<sup>st</sup> July 2025**

## Safe To Host Certificate

<b>Certificate Number</b>	: 047/25-26/1501
<b>Organization Name</b>	: Consulate General of India, Jaffna, Sri Lanka.
<b>Address</b>	: 14 Maruthady Lane, Nallur, Jaffna (Sri Lanka)
<b>Application Name</b>	: Consulate General of India, Jaffna, Sri Lanka.
<b>Production URL</b>	: <a href="https://www.cgijaffna.gov.in/">https://www.cgijaffna.gov.in/</a>
<b>Audit Period</b>	: 1 <sup>st</sup> May 2025 to 31 <sup>st</sup> July 2025
<b>Compliance Verification Date</b>	: 30 <sup>th</sup> July 2025
<b>Hash Value</b>	: 27BCF73837644D9D016F125AADFB410A341E3E8F4878A85C 34E3B82B8E503458.
<b>Path</b>	: /home/cgijaffn/
<b>Certificate Validity</b>	: 1 year (Valid till 29 <sup>th</sup> July 2026)

The above web application has undergone through IT (Cyber) Security Audit by our organization through provided 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: On the basis of audit outcomes, it is certified that the above application is safe 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.
2. Web Application should comply with Guidelines for Secure Application Design, Development, Implementation & Operations issued by CERT-In.
3. Organization must comply with the Directions issued by CERT-In (Notification No. 20(3)/2022-CERT-In) dated 28 April 2022 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.
4. Auditee must also follow the Technical Guidelines on SBOM | QBOM & CBOM | AIBOM | HBOM | Version 2.0 issued by CERT-In dated 09.07.2025

Hausika Soni

**Prepared By & Verified By**  
**DRCBS-24-040 & DRCBS-24-045**



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