IHUB NTIHAC FOUNDATION
CIN- U85300UP2020NPL134133
Registered Office: C3i Building, I.I.T. Campus, Kalyanpur, Kanpur-208016, U.P. India

Application Code Review Closure Certificate

IHUB NTIHAC Foundation, a CERT-In–empanelled cybersecurity auditing organization, hereby certifies that it has conducted an Application Source Code Security Review Kanpur on the web application www.iitk.ac.in, as per the scope agreed upon for this engagement.

The assessment was carried out using a white-box methodology, involving structured manual review of the application source code and relevant configuration artifacts provided for assessment, with the objective of identifying security vulnerabilities, insecure coding practices, logical flaws, and deviations from secure development standards. The review was performed in a controlled and secure assessment environment and was limited to the in-scope components made available for evaluation. The findings and recommendations provided in the report are based on the application state at the time of assessment.

This assessment was conducted in accordance with CERT-In Secure Coding Guidelines and recognized industry best practices, including the OWASP Secure Coding Practices, OWASP Top 10 (2021), and SANS Secure Software Development Guidelines. This certificate confirms the completion of the Application Source Code Review activity for the specified scope and does not constitute a guarantee of absolute security. A Summary of the application code review is mentioned in the Table below:

SNo.	Name of the Applications	Report Submission Date
1.	iit-K-vapt-testing.zip	Evaluation Date – 3rd Nov 2025
		Revalidation I Date – 24th Nov 2025
		Revalidation II Date – 17th Dec 2025
		Revalidation III Date – 6th Jan 2026
		Revalidation IV Date – 16th Jan 2026

Disclaimer:

This certificate is issued based on a **static application source code security review** conducted on the source code and documentation provided for assessment, under controlled conditions and within the agreed scope.The review identified **four security vulnerabilities**, including issues mapped to **OWASP Top 10 (2021)** categories and relevant **CWE classifications**. While **risk-based remediation recommendations** have been provided, these vulnerabilities **remain open at the time of issuance** and therefore represent **residual security risk**. Issuance of this certificate **confirms completion of the source code review activity only** and **does not certify the application as fully secure**, nor does it imply absence of vulnerabilities. This certificate is valid **as of the date of assessment** and may be rendered invalid upon any change to the source code or application configuration.

Issue date – 10th Feb 2026

Dr. Anand Handa
C3iHub, IIT Kanpur