जम्मू एवं कश्मीर ग्रामीण बैंक
JAMMU AND KASHMIR GRAMEEN BANK
Scheduled Bank Owned by Government
Head Office: Near Fruit complex Narwal, Jammu-180006
Ph: 8899006459 / 9103995267 **Email_Id:** dac.hoj@jkgb.bank.in
Digital and Alternate Channels Cell

Ref No : JKGB/DAC/2026-27/5953 *Date: 04-Nov-2026*

CORRIGENDUM-II

This Corrigendum-II is hereby issued in reference to the Request for Proposal (RFP) bearing Reference No. JKGB/DAC/2026-27/5065 dated 01 Oct 2026, for the purpose of incorporating the amendments / clarifications specified herein. **The last date for the submission of bids, i.e. 04 Nov 2026 is hereby extended up to 11 Nov 2026, 05:00 PM**. The following clause-wise amendments / clarifications set forth in this Corrigendum shall form an integral part of the RFP. All other terms and conditions of the RFP shall remain unchanged and continue to be applicable.

Sl. No.	RFP Section / Annexure	Clause / Reference	Original Clause (as per RFP)	Amendment / Clarification
1.	Annexure 2, Point 13, Section E, Clause 3.3.1(A), S.No. 7 All other Provisions/References/Clauses/Sections/Annexures in the RFP relating to NCCRP/I4C.	Technical Experience and Capabilities	NCCRP/I4C Reporting System (Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / Suspect Registry/DPIP/ I4C integration) should have been implemented by the bidder and it is running in real time in at least One Scheduled Public/Private Sector Bank (Including RRBs) in India with at least 300 branches, at least for a period of last Two years as on the date of RFP.	NCCRP/I4C Reporting System (Cross Channel Control Platform including Cyber Complaint Processing, CCCP / NCRP / Suspect Registry/DPIP/ I4C integration) should have been implemented by the bidder and it is running in real time in at least One Scheduled Public/Private Sector Bank (Including RRBs) in India with at least 150 branches, at least for a period of Six (06) Months as on the date of RFP.

2.	Annexure 8 Clause 2.70.52	Application / Solution and API Security	New Clause	The solution shall implement additional application-level security controls, including configurable endpoint-wise IP allow listing with the facility for the Bank to manage approved source IP addresses, protection against SQL/NoSQL Injection, Cross-Site Scripting (XSS), command injection, EDR, Server-Side Request Forgery (SSRF), request tampering and replay attacks. It shall support rate limiting, throttling and protection against brute-force attacks and excessive API requests. Multi-Factor Authentication (MFA) shall be supported for administrative and privileged user access. The solution shall ensure secure storage and management of API credentials, keys and secrets, prevent hardcoding of credentials in application code, and support secure application configuration and hardening by disabling default accounts and unnecessary services. The bidder shall be responsible for implementing and maintaining these controls throughout the contract period.
3.	Corrigendum-I bearing Ref. No. JKGB/DAC/2026-27/5675 dated 21.10.2026, S.No.15 – Onsite Resources	ONSITE RESOURCES	Clarification	It is hereby clarified that the provision is intended solely for providing support and undertaking solution enhancements or further development activities after the go-live of the project.