THE KANGRA CENTRAL CO-OPERATIVE BANK LTD.
कांगड़ा केन्द्रीय सहकारी बैंक सीमित
Head Office, Civil Lines, Dharamshala, Distt. Kangra, H.P. - 176 215, Ph:01892-223280, 224607

RFP No. KCCB/DC/2026/01 Dated 22/04/2026

PROPOSAL FOR DATA CENTER/DR SITE collocation, TRANSPORTATION, INSURANCE & MANAGED SERVICES

The Kangra Central Cooperative Bank Ltd. Dharamshala

Sehkar Jyoti Building, Civil Lines, Dharamshala,
Teh. Dharamshala, Distt. Kangra, Himachal Pradesh, 176 215, India.

Phone Nos.: +91 1892 – 224969 / 222677 / 223280 / 222353 / 222326
Email: it@kccbhp.bank.in
Website: https://www.kccbhp.bank.in/

To,
All the vendors concerned.

Subject: Proposal For Data Center collocation, Transportation, Insurance & Managed Services.

1. INTRODUCTION

The Bank currently operates its Data Centre at Head Office, Dharamshala, and its Disaster Recovery Centre (DRC) at Bengaluru. The Bank has been migrating its Core Banking Solution (CBS) and allied applications to a Hybrid Data Centre model, comprising:

- Physical Data Centre at Head Office, Dharamshala
- Cloud Data Centre at AWS Mumbai (Sify Data Center – Rabale, Mumbai)
- Cloud Disaster Recovery Data Centre at AWS Hyderabad (GPX Data Center – Hyderabad)

Pursuant to this transition, the existing Disaster Recovery Centre at Bengaluru is proposed to be decommissioned. Consequently, the IT infrastructure and devices presently hosted at the Bengaluru DRC are required to be relocated either to the Physical Data Centre at Dharamshala or to the Cloud Disaster Recovery Data Centre at AWS Mumbai. In addition, certain devices currently hosted at the Physical Data Centre, Dharamshala, are proposed to be relocated to the AWS Hyderabad location. In view of the above, the Bank requires colocation facilities at Mumbai and Hyderabad, with seamless and secure connectivity to AWS

For hosting the identified devices (Annexure III) at AWS Hyderabad, AWS Mumbai and/or Dharamshala, the Bank requires comprehensive collocation Services, which shall include, but not be limited to:

- Provisioning of standardized rack space
- Redundant power supply along with associated electrical and cooling infrastructure
- Secure transportation of devices from Bengaluru/Dharamshala to the designated collocation facilities, including transit insurance coverage
- Managed services for installation, configuration, monitoring, and ongoing operational support.
- Provision of dedicated cross-connect connectivity between the collocated devices and the respective AWS racks at Mumbai and/or Hyderabad to ensure seamless integration with the Bank's cloud environment.

The collocation facilities must ensure minimum service availability of 99.99%, supported by appropriate SLAs, redundancy, and monitoring mechanisms.

Accordingly, the Bank proposes to procure suitable collocation services at the following locations to facilitate the safe migration, hosting, and management of its IT infrastructure, in alignment with its hybrid data centre strategy:

- Sify Data Center – Rabale, Mumbai
- GPX Data Center – Hyderabad

The objective is to establish a secure, scalable, and fully managed collocation environment with standardized capacity, high availability, and consistent operational support across all sites.

2. SCOPE OF SERVICES

2.1. Collocation Services

Each Data Center location will provide the following minimum infrastructure:

S No	Parameter	Specification
1	Rack Space	Minimum 25U (Dedicated Rack Space)
2	Power Allocation	Minimum 5 kVA
3	Power Redundancy	N+1 / 2N (as per DC standards)
4	Power Distribution	Redundant PDUs
5	Cooling	Precision Air Conditioning
6	Physical Security	24x7 CCTV, Biometric / Access Card
7	Fire Protection	VESDA & Gas-Based Suppression
8	Compliance	ISO 27001 / SOC / PCI-DSS (as applicable)
9	Insurance	Hosted devices must be covered under insurance

2.2. Data Center Locations

S No	Location	City	Data Center Provider
1	Location 1	Mumbai (Rabale)	Sify Data Center
2	Location 2	Hyderabad	GPX Data Center

3. TRANSPORTATION & INSURANCE COVERAGE

3.1. Transportation

- Door-to-data-center transportation
- Secure, sealed vehicles
- Handling by trained professionals
- Equipment delivery confirmation at site

3.2. Insurance Coverage

- Comprehensive insurance during transit
- Coverage includes:
    - Loss
    - Theft
    - Physical damage
- Insurance value based on **declared equipment cost**

4. MANAGED SERVICES (ALL LOCATIONS)

4.1. Remote Hands & Smart Hands

- Rack and stack support
- Cable management
- Power cycling and reboot support
- Media replacement assistance
- Visual inspections

4.2. Monitoring & Support

- 24x7 monitoring
- Power and environmental monitoring
- Incident management and escalation
- Coordination with OEMs / ISPs if required

4.3. Service Levels

- 24x7 operational support
- CCTV surveillance storage of footage minimum up to 180days.
- Defined response and resolution timelines
- Monthly service reporting

5. TAXES & PAYMENT TERMS

- Prices are exclusive of applicable taxes
- GST will be charged as per government norms
- **Schedule of Payment**
  - No payment will be made in advance.
  - 100% one-time charges for Transportation, Insurance shall be released after successful delivery.
  - 100% one-time charges for implementation shall be released after successful installation, configuration, integration, implementation , testing and submission of installation reports and other documents.
  - All costs for services like support/maintenance etc. shall be released on quarterly basis upon raising of relevant invoices at the end of the concerned quarter.

6. OTHER TERM & CONDITIONS

1. The rates shall be valid for Three (3) years.
2. The duration of the project shall be three years from the date of purchase order, to be renewed, subject to the performance of the Service Provider on year-to-year basis.
3. It is a single envelope bid system. Service Providers shall enclose: -
   - Copy of valid PAN No. & GST registration certificate.
   - Duly signed pages of proposal document.
   - Duly filled and signed Annexures I.
   - Duly filled and signed price bid as per Annexure-II.
4. Commercials should be neatly typed on the letter head of the Service Provider, duly filled in, signed and complete as per the prescribed Proforma as given in ANNEXURE -II.
5. The L1 Service Provider shall be arrived at by considering the consolidated rate quoted in the Proforma Commercial Bid as given in ANNEXURE – II. The one-time charges towards transportation and insurance quoted by the selected L1 service provider shall be treated as final.
6. Proposal filled in all respect shall be sealed in an envelope and super scribed as "**: Proposal For Data Centre collocation, Transportation, Insurance & Managed Services** FOR THE KANGRA CENTRAL COOPERATIVE BANK LTD. DHARAMSHALA." **OR** Through email enclosing Quotation as a password protected file and password to be communicated over phone at the time of opening the quotations.
7. Sealed/Password protected quotations shall be submitted on or before 30/04/2026 at 11:00 AM addressed to "The General Manager, The Kangra Central Cooperative Bank Ltd. Head Office Dharamshala" or shall be sent to email id it@kccbhp.bank.in.
8. The quotations will be opened by a committee on the same day at 3.00 PM. The Bank will not be responsible for delay in submission of quotations sent by post.
9. The quotation will be remained valid for acceptance for a period of 60 days from the date of receipt by the Bank.
10. Incomplete and ambiguous quotations shall be rejected.

11. The Bank reserves the right to accept / reject any quotation without assigning any reason.

12. The rates shall be in whole numbers. The rates shall be entered in figures as well as in words. For the purpose of the quotation, the metric system of units shall be used. In the event of any discrepancy, the rates quoted by the vendor in words will be taken as the correct basis and not the rates shown in figures.

13. The person(s) signing the bid, with date, shall sign all changes, alterations, and corrections in the bid in full (if necessary).

14. Quotation, in which any of the particulars and prescribed information are missing or are incomplete, in any respect and /or prescribed conditions are not fulfilled, shall be considered nonresponsive and are liable to be rejected.

15. No correspondence shall be entertained from the vendors after the opening of the Quotation.

16. Date of acceptance and opening of quotation can be extended on the sole discretion of the Bank.

17. The competent authority of this office reserves the right to reject/cancel any quotation or all quotations without assigning any reasons.

18. To ensure efficient and effective rollout of the project as well as to ensure smooth operations of the complete system during the entire project life, the Service Provider will be required to work in collaboration with any agency/service provider involved with Bank.

19. The service provider shall make the proposed collocation site at Mumbai ready in the first phase and shall complete site readiness within a maximum period of 30 days. In parallel, the service provider shall undertake site readiness activities at the proposed collocation site in Hyderabad.

20. INDEMNITY AND LIMITATION OF LIABILITY

1. The Service Provider shall, at their own expense, defend and indemnify the Bank against all third-party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial design rights arising from use of the supplied/delivered products/services on licensing, violation or non-compliance to statutory regulations and guidelines in India or abroad.
2. The Service Provider shall expeditiously extinguish any such claims and shall have full rights to defend itself there from. If the Bank is required to pay compensation to a third party resulting from such infringement, the Service Provider shall be fully responsible therefore, including all expenses and court and legal fees.
3. The Bank will give notice to the Service Provider of any such claim without delay, provide reasonable assistance to the Service Provider in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim.
4. Notwithstanding anything under this agreement Service Provider's total liability to the bank for all claims, in the aggregate, under or in connection with this contract will be limited to maximum to the purchase order value.

21. CONFIDENTIALITY

1. The Service Provider shall not, and without the Bank's prior written consent, disclose the contract or any provision thereof, or any specification, plan, drawing,

pattern, sample or information furnished by or on behalf of the Bank in connection therewith to any person other than a person employed by the Service Provider in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

2. The Service Provider shall not without the Bank's prior written consent, make use of any document or information for the purpose other than that specified in the agreement.
3. Any document other than the contract itself shall remain the property of the Bank and shall be returned (in all copies) to the Bank on completion of the Service Provider's performance under the contract if so required by the Bank.
4. The Service Provider shall be responsible for any loss caused by disclosure of any above said confidential material.

22. FORCE MAJEURE DURING THE PENDENCY: During the pendency of the contract if the performance in whole or part thereof by either party is prevented / delayed by causes arising due to any war, hostilities, civil commotion, act of public enemy, sabotage, fire, floods, explosion, epidemics, non-availability of raw material, and other consumables, or any other causes including breakdown of equipment beyond their reasonable control neither of the two parties shall be made liable for loss or damage due to delay or failure to perform the contract during the pendency of forced conditions provided that the happenings are notified in writing within 7 days from the date of occurrence. The work shall be resumed under the contract as soon as possible after resumption of normalcy.

23. ARBITRATION: All disputes, differences, claims and demands arising under or pursuant to or touching the contract shall be referred to the sole arbitrator to be appointed mutually by both parties. The award of the sole arbitrator shall be final and binding on both the parties under the provisions of the Arbitration and Conciliation Act, 1966 or by statutory modification/re-enactment thereof for the time being in force. Such arbitration shall be held at Dharamshala.

24. JURISDICTION OF COURTS: In all matters and disputes arising there under, the appropriate Courts at Dharamshala, or any competent court within the territory of H.P. shall have the jurisdiction to entertain and try them.

25. The Service Provider should comply with Digital Personal Data Protection (DPDP) Act, 2023.

26. The service provider shall comply with RBI Guidelines RBI/2021-22/64 DOR.ORG.REC.27/ 21.04.158/ 2021-22 dated 28.06.2021 regarding Guidelines for Managing Risk in Outsourcing of Financial Services by Cooperative Banks and RBI/DPR/2025-26/318 DOR.ORG.REC.No.237/21-04-158/2025-26 dated 28/11/2025 on Managing Risks in Outsourcing) Directions, 2025.

27. As per RBI circular RBI/2019-20/129DoS.CO/CSITE/BE.4083/31.01.052/2019-20 dated 31.12.2019 and NABARD circular no NB.DoS.Pol.HO/3182/J-1/2019-20 dated 06.02.2020, the following changes are required:

1. The service provider have to get themselves annually audited by external empanelled Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/software) and

services etc. provided to the Bank and the Service Providers are required to submit such certification by such Auditors to the Bank.

2. The service provider and or his / their outsourced agents / sub –contractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. Service Provider shall, whenever required by the Auditors, furnish all relevant information, records/data to them. Where any deficiency has been observed during audit of the Vendor on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, the Vendor shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by the Service Provider shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.
3. Service Provider shall, whenever required by the Bank, furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/Reserve Bank of India and or any regulatory authority. The Bank reserves the right to call and/or retain for any relevant material information / reports including audit or review reports undertaken by the service provider (e.g., financial, internal control and security reviews) and findings made on Service Provider in conjunction with the services provided to the Bank.

28. The Roles & Responsibility in case of cyber incident will be vide RBI circular RBI/2015-16/418 DBS.CO. CSITE/ BC.11/ 33.01.001/ 2015-16 dated 02.06.2016, RBI/2018-19/63 DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 dated 19.10.2018 and NABARD circular no. 50/DoS-16/2018 dated 16.03.2018 are defined in CCM (Cyber Crisis Management Plan) of the Bank. The Roles & Responsibility for vendor and the Bank in case of cyber incident, but not limited to, are as under: -

1. **Containment:** Containment has two goals:
   - Prevent data from leaving the network via the affected machines. (Bank or Vendor or Both)
   - Prevent attacker from causing further damage to information technology assets (Bank or Vendor or Both)

   The following actions are taken during the containment phase:
   - To proceed to repair the system as needed to return to normal business operations. (Bank or Vendor or Both)
   - Securing the physical area on site if necessary. (Bank or Vendor or Both)
   - A review of the information provided by the system administrators. (Bank or Vendor or Both)
   - Not allowing the affected system to be altered. (Bank or Vendor or Both)
2. **Eradication:** The general steps involved in the eradication phase of incident response are to:
   - Identify and mitigate all vulnerabilities that were exploited. (Bank or Vendor or Both)
   - Remove malware, inappropriate materials, and other components. (Bank or Vendor or Both)
   - If more affected hosts are discovered, repeat the Detection and Analysis steps to identify all other affected hosts, then contain and eradicate the incident for them. (Bank or Vendor or Both)

- Reinstall OS, apply patches, reinstall applications and apply known patches. (Bank or Vendor or Both)

3. **Recovery:** Once the incident has been contained and eradicated, recovery can start. This phase allows business processes affected by the incident to recover and resume operations. The general recovery steps are:
   - Reinstall and patch the OS and applications. Change all user and system credentials. (Bank or Vendor or Both)
   - Restore data to the system. (Bank or Vendor or Both)
   - Return affected systems to an operationally ready state. (Bank or Vendor or Both)
   - Confirm that the affected systems are functioning normally. (Bank or Vendor or Both)
   - If necessary, implement additional monitoring to look for future related Post-Incident Activity. (Bank or Vendor or Both)
4. **Incident Closure:** Documentation of a cyber-incident and the steps taken to mitigate issues encountered shall be reported to the Board as well as with the other stake holders, controllers and regulators as deemed appropriate. The Incident Closure document may contain:
   - Information about the incident type. (Bank or Vendor or Both)
   - A description of how the incident was discovered. (Bank or Vendor or Both)
   - Information about the systems that were affected. (Bank or Vendor or Both)
   - Information about who was responsible for the system and its data. (Bank or Vendor or Both)
   - A description of what caused the incident. (Bank or Vendor or Both)
   - A description of the response to the incident and whether it was effective. (Bank or Vendor or Both)
   - Recommendations to prevent future incidents. (Bank or Vendor or Both)
   - A discussion of lessons learned that will improve future responses. (Bank or Vendor or Both)
   - A timeline of events, from detection to incident closure. (Bank or Vendor or Both)

The General Manager

The Kangra Central Coop. Bank Ltd.

Head office Dharamshala

I AM ACCEPTING ALL THE TERMS & CONDITIONS OF THE BANK MENTIONED ABOVE WITHOUT ANY PREJUDICE.

(SIGNATURE & SEAL OF SERVICE PROVIDER)

ANNEXURE-I

PROFORMA OF LETTER FOR E-PAYMENT

To

The General Manager,
The Kangra Central Cooperative Bank Ltd.
Head Office Dharamshala-176215

Subject: Request for E-Payment.

Sir,

Following particulars are given for effecting E-payment in respect of our claim / Bill.

1. Name of the Company:
2. Address:
3. Bank A/c number:
4. Name of Bank / Branch & Address:
5. Branch Code:
6. IFSC Code of the Bank:
7. PAN of the Company:
8. Mobile No. of the Account Holder:

We also enclose herewith a cheque duly cancelled of our bank A/c.

Thanking You.

Yours Faithfully

(Authorized Signatory)

Note: Any erroneous information may lead to harmful transaction for which the Bank will not be liable / responsible.

ANNEXURE -II

COMMERCIALS:

A. One-Time Charges: Transportation & Insurance Charges:

S No	Location	Transportation Charges (i)	Insurance Charges (ii)	Total (i +ii)
1	Bengaluru => Mumbai			
2	Bengaluru => Dharamshala			
3	Dharamshala => Hyderabad			

B. Project Cost:

S No	Location	One Time Cost (a)	Annual Recurring Charges (b)				Total (a+b) (Criterion for declaring L1)
		Implementation Charges	Collocation Charges (i)	Managed Services Charges (ii)	Cross connect Charges(iii)	AWS Direct connect Charges(if any) -200Mbps (iv)	
1	Sify DC – Mumbai						
2	GPX DC – Hyderabad						

ANNEXURE -III

LIST OF ITEMS TRANSPORTED

S No	Device	Qty	Total Value	Existing Location	Transported to Location
1	Blade Chassis	1	1,50,115	Whitefield Bengaluru	Dharamshala
2	Blade Servers	7	1,25,640		Dharamshala
3	SAN Storage (IBM V3700)	1	7,92,822		Dharamshala
4	HSM (Gemalto)	2	1,00,000		Dharamshala
5	KVM Switch	1	26,003		Dharamshala
6	KVM Console (Monitor, Keyboard, Mouse)	1	85,153		Dharamshala
7	Media Converter	2	2,000		Dharamshala
8	Cisco MDS 9148S SAN Switch	2	1,00,000		Dharamshala
9	PDU	2	25,000		Dharamshala
10	NVR with Camera	1	43,500		Dharamshala
11	Router-NPCI	1	35,000		Dharamshala
12	Cisco Catalyst 3560_Bank	1	1,50,000		Dharamshala
13	Switch (unmanaged) - I	1	1,000		Mumbai
14	HSM (Thales)	2	62,76,048		Mumbai
15	Firewalls	2	10,41,862		Mumbai
16	Cisco 4200 Series Router_Sarvatra	2	1,70,000		Mumbai
17	Router -NPCI	2	7,25,786		Mumbai
18	Switch- NPCI	2	2,80,968		Mumbai
	Total*	33			

S No	Device	Qty		Existing Location	Transported to Location
1	HSM (Thales)	2	62,76,048	Dharamshala	Hyderabad
2	Cisco 4200 Series Router_Sarvatra	2	1,70,000		Hyderabad
3	Switch_NPCI	2	2,76,000		Hyderabad
4	Router_NPCI	2	6,63,562		Hyderabad
	Total	8			

* In case some additional items installed by Bank, may also be included in this proposal.