KERALA STATE ROAD TRANSPORT CORPORATION

TRANSPORT BHAVAN, FORT, THIRUVANANTHAPURAM-695 023

Telephone No: 0471-2471011, (Extn : 250)

E-mail: edpc.krtc @kerala.gov.in Web: www.keralartc.com

No. S001-ITD01/34/2026-ITDIV -KSRTC-HQ **Date: 02.09.2026**

CORRIGENDUM – 2

Tender ID :	**2026_KSRTC_865917_1**
Tender Reference Number :	**ITD01/34/2026**
Tender Title :	**PROCUREMENT OF CLOUD SERVICES FROM MeitY EMPANELLED CLOUD SERVICE PROVIDERS**

TECHNICAL CORRIGENDUM-Amendments to the Tender Document

The following amendments are made to the Tender Document. Column 3 reproduces the provision as originally published and column 4 sets out the provision as amended.

Item	Provision amended	As originally published	As amended
B-1	Cover page; Section I, second paragraph; Bid Data Sheet, Section I; Section II, Clause 6; Section II, Clause 3, item 8; Form 1, paragraph 8; Form 6; Annexure C, Cover A, item 9	Cover page legend reads "TWO-COVER SYSTEM | ONLINE BIDDING ONLY | NO EARNEST MONEY DEPOSIT". Section I, second paragraph reads "Participation requires no Earnest Money Deposit and no tender document fee; a Bid Securing Declaration in the prescribed format is accepted in lieu of Earnest Money Deposit." The Bid Data Sheet nevertheless shows a tender document fee of Rs.5,900/- and an Earnest Money Deposit of Rs.1,00,000/-.	The internal inconsistency is resolved in favour of the Bid Data Sheet and of the particulars published on the e-GP Portal. (a) The words "| NO EARNEST MONEY DEPOSIT" on the cover page are deleted. (b) The second paragraph of Section I is substituted by: "Participation requires payment of the tender document fee and of the Earnest Money Deposit shown in the Bid Data Sheet, online through the e-GP Portal. A Bidder entitled to exemption from the Earnest Money Deposit under the orders of the Government of India or of the Government of Kerala in force shall upload the valid exemption certificate together with the Bid Securing Declaration in Form 6, in lieu of the Deposit." (c) In the Bid Data Sheet, against 'Tender document fee' read: "Rs.5,900/- (Rs.5,000/- + GST at 18%), together with the e-GP Portal processing fee of Rs.295/-, aggregating Rs.6,195/-, payable online only." Against 'Earnest Money Deposit' read: "Rs.1,00,000/- (Rupees One Lakh only), payable online through the e-GP Portal; exemption admissible against a valid certificate." (d) Form 6 shall be submitted only by a Bidder claiming exemption from the Earnest Money Deposit, and its heading is amended accordingly. (e) In Section II, Clause 3, item 8 and in Annexure C, Cover A, item 9, read: "Proof of online remittance of the Earnest Money Deposit; or, where exemption is claimed, the

Item	Provision amended	As originally published	As amended
			exemption certificate together with the Bid Securing Declaration in Form 6." (f) In Form 1, paragraph 8, read: "We have remitted the tender document fee and the Earnest Money Deposit online through the e-GP Portal / We claim exemption from the Earnest Money Deposit, and have furnished the exemption certificate and the Bid Securing Declaration in Form 6. *[Strike out whichever is not applicable.]*" (g) Wherever the Tender Document provides for the enforcement of the Bid Securing Declaration, it shall be read as providing, in the case of a Bidder that has furnished an Earnest Money Deposit, for the forfeiture of that Deposit.
B-2	Bid Data Sheet, Section I; Section II, Clause 6, first paragraph; Form 1, paragraph 7	"Bids shall remain valid for ninety (90) days from the last date of submission."	For "ninety (90) days" read "one hundred and eighty (180) days", wherever the expression occurs in relation to the validity of Bids. The consequential period of forty-five (45) days for the expiry of the Bid Securing Declaration is unaltered.
B-3	Section II, Clause 5.3; Section V, Note 8 to the Bill of Quantity	"the Bidder shall quote at a conversion rate of 1 USD = Rs. ______ *[to be filled in by KSRTC at the time of publication]*"	For the blank read: "1 USD = Rs.94.94 Every Bidder shall use this single rate, and no claim on account of exchange-rate fluctuation shall be entertained.
B-4	Annexure B, closing paragraph	"The aggregate data presently held across these workloads is of the order of ______ TB *[to be filled in by KSRTC at the time of publication]*, and the peak concurrent user load on the public-facing systems is of the order of ______ *[to be filled in]*."	For the blanks read: aggregate data of the order of 5 TB, and a peak concurrent user load on the public-facing systems of the order of 2***k users*** These figures remain indicative and are furnished for sizing only; they are not a warranty, and invoicing shall in all cases be on actual consumption.
B-5	Annexure A, requirement 10; Section V, Storage — the two block volume line items	"Persistent block storage volumes are offered on NVMe or SSD media, supporting a baseline of not less than 30 IOPS per GB for application volumes and not less than 60 IOPS per GB for database volumes."	Substituted by: "Persistent block storage volumes are offered on NVMe or SSD media, supporting a baseline of not less than 6 IOPS per GB, subject to a minimum of 3,000 IOPS for each application volume and of 5,000 IOPS for each database volume, and a higher performance tier is available on demand." In Section V, for "not less than 30 IOPS per GB" read "not less than 6 IOPS per GB, minimum 3,000 IOPS per volume", and for "not less than 60 IOPS per GB" read "not less than 6 IOPS per GB, minimum 5,000 IOPS per volume". Where KSRTC requires a higher performance tier during the Contract, it shall be provisioned under Clause 8 of Section IV.
B-6	Annexure A, requirement 11	"The capacity of a provisioned volume may be increased on demand without rebooting the virtual machine, and the IOPS of a volume may be increased dynamically without changing the size of the volume."	Substituted by: "The capacity of a provisioned volume may be increased on demand without rebooting the virtual machine, and the IOPS of a volume may be increased without changing the size of the volume. Where the guest operating system requires a restart in order to recognise a change in capacity or in performance, the restart shall be carried out in a maintenance window notified and approved under Clause 6.1 of Section IV, and the resulting downtime shall be excluded from the computation of availability."
B-7	Annexure A, requirement 12; Section IV, Clause 3.3	"…with the option of customer-managed keys held in a key management service backed by a	Substituted by: "…with the option of customer-managed keys held in a key management service. Where the Cloud Service Provider

Item	Provision amended	As originally published	As amended
		hardware security module certified to FIPS 140-2 Level 3 or higher.”	offers a dedicated hardware security module service, that service shall be certified to FIPS 140-2 Level 3 or higher. Where the Cloud Service Provider does not offer a dedicated hardware security module service, a key management service in which customer-managed keys are held in cryptographic modules certified to FIPS 140-2 Level 2 or higher shall be acceptable.” No key management service is required to be priced in the Financial Bid; if KSRTC elects to use customer-managed keys, the service shall be provisioned under Clause 8 of Section IV at the published list price of the Cloud Service Provider, less the Additional Services Discount quoted.
B-8	Annexure A, requirements 20, 22 and 25; Section V, the Web Application Firewall, Security monitoring and Managed threat detection line items	Requirements and line items requiring the capability to be a “native service of the Cloud Service Provider” or “native”.	The following general rule is inserted at the head of Annexure A and shall govern Section V correspondingly: “Wherever a capability is required to be a native service of the Cloud Service Provider, it is sufficient that the capability is delivered on the platform of the Cloud Service Provider, is provisioned within the tenancy owned by KSRTC, is configured and managed by the Contractor through the same operations console and ticketing system as the rest of the estate, is billed under this Contract, and involves no storage, processing or transfer of the data of KSRTC outside India or outside the control of the Contractor. Requirement 20 (object storage, caching and application programming interface gateway), requirement 22 (web application firewall) and requirement 25 (security information and event management, managed threat detection, automated security assessment and cloud security posture management) shall be read accordingly.” The obligations of the Contractor as to audit (Clause 9 of Section IV), data ownership (Clause 9 of Section III) and exit (Clause 10 of Section IV) extend to every such service.
B-9	Section VI, Clause 2, criterion 6; Section II, Clause 3, item 10; Annexure C, Cover A, item 7; Form 3, Part B	“The Bidder shall have on its rolls not fewer than three (3) technical resources holding a current certification of the proposed Cloud Service Provider at associate level or above.” Documentary evidence: “Statement of resources with certification identifiers and validity, signed by the authorised signatory.”	Substituted by: “The Bidder shall have on its rolls not fewer than three (3) technical resources holding a current cloud certification at associate level or above, being either a certification of the proposed Cloud Service Provider or, where the proposed Cloud Service Provider does not operate a certification programme, a certification of Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure or IBM Cloud. Where the proposed Cloud Service Provider does not operate a certification programme, a declaration to that effect on its letterhead shall be furnished with Form 5.” Documentary evidence: the statement at Part B of Form 3, giving for each resource the name, the certification held and its level, the certification identifier and the validity, signed by the authorised signatory. Copies of individual certificates need not be uploaded with the Bid; KSRTC may verify any certification identifier on the public verification facility of the certifying body and may call for the certificate at any stage. Item 7 of Cover A in Annexure C is amended accordingly.

Item	Provision amended	As originally published	As amended
B-10	Section IV, Clause 3.2; Section V, the Disaster recovery replication line item and column D generally	"The Contractor shall set up and configure the virtual machines, storage, network and database at the Disaster Recovery site so as to meet a Recovery Point Objective of thirty (30) minutes and a Recovery Time Objective of four (4) hours. When the Disaster Recovery site is made active, it shall provide not less than the capacity and functionality of the Data Centre."	The following is added after the words "capacity and functionality of the Data Centre": "The Disaster Recovery architecture shall be active-passive. Replication of data shall be continuous, so as to meet the Recovery Point Objective of thirty (30) minutes at all times, and the storage required to hold the replicated copy of the entire estate shall be provisioned at the Disaster Recovery site at all times. The compute capacity at the Disaster Recovery site may be maintained in a reduced state, provided that capacity and functionality not less than that of the Data Centre is made available within the Recovery Time Objective of four (4) hours, and provided that this is demonstrated in each half-yearly disaster recovery drill. Compute instantiated at the Disaster Recovery site for a drill, a test or a declared disaster shall be billed on actual consumption at the unit rates quoted for the corresponding compute line items." In Section V, the indicative quantities in column D relate to the Data Centre; against the line item 'Disaster recovery replication to the DR site' add: "inclusive of all replication software, licences and services and of the storage required at the Disaster Recovery site for the replicated copy of the entire estate; compute at the Disaster Recovery site is not included in this lot."
B-11	Section V, Security — 'Managed threat detection', column D	Indicative quantity: 15 (Per VM / month).	For "15" read "17", being the fourteen (14) virtual machines and the three (3) managed database deployments shown in this schedule. This corrects an arithmetical inconsistency pointed out at the pre-bid stage.
B-12	Section IV, Clause 3.2, second paragraph	"The Contractor shall not delete any data during the Contract period without the written approval of KSRTC…"	The following proviso is added: "Provided that the expiry of a backup copy in the ordinary course, on the completion of the retention period fixed in the backup policy approved by KSRTC, shall not constitute deletion of data for the purposes of this clause. The requirement of prior written approval applies to the deletion of primary data, to the deletion of any backup copy before the expiry of the approved retention period, and to any change in the approved retention policy."
B-13	Section IV, Clause 3.4 (new paragraph)	The clause does not at present allocate responsibility for changes at application level.	The following paragraph is inserted: "The Contractor is responsible for the landing zone, for the provisioning and configuration of compute, storage, network, database and security services, for the build and upgrade of operating systems to a currently supported version, for the migration of virtual machines, databases and data, for cut-over and rollback, and for joint testing. Changes at application level — refactoring of application code, conversion of database schema, compatibility fixes and the re-deployment of application binaries — remain the responsibility of the respective application vendors of KSRTC, and the Contractor shall coordinate with those vendors, provide the environments and access required, and support the joint acceptance testing. Where an operating system must be upgraded in the course of migration, the Contractor shall provide the upgraded

Item	Provision amended	As originally published	As amended
			operating system and the application vendor shall re-deploy the application upon it.”
B-14	Section IV, Clause 5, Milestone 3	“Migration of applications, databases and data, with full functionality on the cloud, including workloads migrated from vendor-operated source environments — Within forty-five (45) working days of the issue of the Purchase Order.”	For the timeline read: “Within sixty (60) working days of the issue of the Purchase Order. Migration may be phased workload by workload in the manner agreed in the migration plan. In respect of a workload whose source environment is operated by a third party, the period shall be reckoned from the date on which administrative access to that source environment is made available to the Contractor, and the outer limit for the migration of all workloads shall be ninety (90) working days from the issue of the Purchase Order.” Liquidated damages under Clause 11 of Section III shall be computed with reference to the timeline as so amended.
B-15	Section VI, Clause 2, criterion 10; Form 1, paragraph 13	“The Bidder shall undertake to establish and maintain, within thirty (30) days of the Letter of Award and throughout the Contract period, a support presence at Thiruvananthapuram, with a named account manager and a named technical single point of contact.”	Substituted by: “The Bidder shall undertake to establish and maintain, within thirty (30) days of the Letter of Award and throughout the Contract period, a named account manager and a named technical single point of contact for KSRTC, and a support presence in the State of Kerala from which a representative of the Contractor is able to attend in person at Transport Bhavan, Thiruvananthapuram within four (4) hours of a call in respect of a Severity 1 incident.” This is without prejudice to Clause 3.4 of Section IV, under which one cloud engineer shall be deployed on site at the Headquarters of KSRTC until the completion of migration.
B-16	Section V, Network — ‘Bastion service for administrator access to private subnets’	“Bastion service for administrator access to private subnets.”	Substituted by: “Bastion service, or an equivalent secure privileged-access service comprising an SSL or IPSec virtual private network together with a hardened jump host, for administrator access to private subnets, with multi-factor authentication and with the recording and logging of every administrative session.”
B-17	Section IV, new Clause 1A; Section I, Clause 2; Section VI, Clause 1 (rider)	The Tender Document records no classification of applications and data, and confines participation to MeitY-empanelled Cloud Service Providers and their authorised partners.	A new Clause 1A is inserted in Section IV: “Classification of applications and data. The applications and data listed at Annexure B have been classified by KSRTC in terms of the National Information Security Policy and Guidelines of the Ministry of Home Affairs, read with Office Memorandum F.No.9(3)/2025-EG-II dated 20.03.2026 of the Ministry of Electronics and Information Technology. The workloads at Annexure B are classified as Category B, Any application or data classified as Category A shall be hosted only in accordance with Option 1 or Option 2 of Table 1 of the said Office Memorandum, and stands excluded from the scope of this Contract until KSRTC directs otherwise in writing.” In Section I, Clause 2, the following is added: “Participation is also open, under the nomination route recognised by paragraph 4(i) of the said Office Memorandum, to the National Informatics Centre, to a State Data Centre, and to a Public Sector Undertaking or other entity under the administrative control of the Ministry of Electronics and Information Technology that has onboarded a MeitY-

Item	Provision amended	As originally published	As amended
			empanelled Cloud Service Provider through the Government e-Marketplace or through an open request for proposal, subject in each case to Section VI." In Section VI, Clause 1, a rider is added: "In the case of a Bidder participating under the nomination route, criterion 1 is satisfied by the empanelment of the Cloud Service Provider that the Bidder has onboarded, and criteria 7 and 8 of Clause 2 shall be read as satisfied by the documents evidencing that onboarding."
B-18	Section V, Managed database line items	"Managed MySQL (PaaS), 8 vCPU / 32 GB RAM, with high availability and automated backup — Per instance / month — 2" and the corresponding PostgreSQL line item.	The following is added to the specification of both line items: "The unit price quoted shall be inclusive of every node, replica, standby instance and licence required to deliver the high-availability configuration offered. The quantity in column D denotes the number of managed database deployments and not the number of nodes." The quantities are not altered.
B-19	Section V, Compute — Linux line items	"Linux VM (non-burstable), 16 / 8 / 4 vCPU…"	The following note is added to the Compute — Linux category: "Linux shall be Ubuntu LTS, Red Hat Enterprise Linux, Rocky Linux or Oracle Linux, in a version currently supported by the publisher. Where a subscription or licence charge arises in respect of the distribution offered, it shall be included in the unit price quoted, and no charge on that account shall be payable separately. The distribution applicable to each workload shall be settled during the discovery exercise."
B-20	Section V, Security — 'Vulnerability scanning of the full estate'	"Vulnerability scanning of the full estate at operating system level, covering missing patches, packages, open ports and CIS compliance — Per month — 1."	The following is added: "This line item covers one automated scan of the full estate in each month. The vulnerability assessment and penetration testing to be conducted twice in each year under Clause 3.3 of Section IV, by an agency empanelled with the Indian Computer Emergency Response Team, is included in the managed services lot and is not separately priced. Its scope is confined to the assets and applications hosted on the cloud under this Contract."
B-21	Section V, Security — 'Security monitoring and compliance — managed SIEM and log analytics'	"Security monitoring and compliance — managed SIEM and log analytics — Per GB / month — 100."	The unit of measurement is retained as 'Per GB / month', so that all Financial Bids remain comparable on a single Total Evaluated Bid Value. The following is added to the specification: "with online retention of logs for not less than ***90*** days and archival retention for not less than ***365*** days, the archival storage being included in the unit price quoted." A Bidder whose Cloud Service Provider prices this service per device shall convert its price to the per-GB unit for the purpose of quoting.
B-22	General	—	Where a provision amended by this Corrigendum is repeated, reproduced or cross-referred elsewhere in the Tender Document, including in the Forms and in Annexure C, the repetition or cross-reference shall be read as amended. Save as expressly amended by this Corrigendum, every other term and condition of the Tender Document remains unaltered and in force.

Part C — Reply to the pre-bid queries

The queries received are set out below in a summarised form, together with the reply of the Corporation. The summary is for convenience of reference only; where a reply refers to an amendment, the text of the amendment at Part B governs. A query that seeks a relaxation which has not been granted is answered accordingly, and the provision concerned stands unaltered.

Q. No.	Reference	Query, in brief	Reply of KSRTC
P-1	Section IV, Clause 1 (Background) — Primenet Global Pvt. Ltd.	Details sought of how the payment gateway used by the ticketing system is integrated with the existing KSRTC infrastructure, and of the connectivity architecture and dependencies.	The reservation and ticketing systems integrate with the payment aggregator over public application programming interfaces on HTTPS. No dedicated or private connectivity to the payment aggregator is required from the cloud environment, and compliance of the aggregator with the Payment Card Industry Data Security Standard remains the responsibility of the aggregator.The interface details will be furnished to the successful Bidder during the discovery exercise, under the Non-Disclosure Agreement in Form 8.
P-2	Section IV, Clause 3.2 — backup retention and deletion	Retention is fixed at not less than thirty days, yet no data may be deleted without prior written approval; clarification sought on the automatic expiry of backups at the end of the retention period.	Accepted. See amendment B-12. The routine expiry of a backup copy at the end of the approved retention period is not 'deletion' and requires no separate approval. Written approval is required for the deletion of primary data, for the deletion of a backup copy before the retention period expires, and for any change in the approved retention policy.
P-3	Section IV, Clause 3.2 — present disaster recovery architecture and management	Details sought of the existing DR architecture (active-active or active-passive) and of whether the infrastructure is managed by KSRTC or by a third party.	There is at present no consolidated disaster recovery arrangement. As stated in Clause 1 of Section IV, the workloads are distributed across on-premises servers at Transport Bhavan, shared hosting and cloud environments provisioned through several intermediaries, and are managed by the respective vendors under separate arrangements, with the IT Division managing the on-premises estate. The architecture to be delivered under this Contract shall be active-passive, as now provided by amendment B-10.
Y-1	Page 19, Section IV, Clause 5 — migration timeline	Migration timelines depend on the number of assets and the volume of data; request to derive the timeline after discovery.	Accepted in part. See amendment B-14: sixty (60) working days, phased workload by workload, with the period reckoned from the date of access in the case of a vendor-operated source environment and an outer limit of ninety (90) working days. The timeline is not left to be fixed after discovery, since it must be common to all Bidders.
Y-2	Page 23, Section V — Compute Linux	Confirmation sought of the Linux distribution required.	See amendment B-19. Ubuntu LTS, Red Hat Enterprise Linux, Rocky Linux or Oracle Linux, in a currently supported version; any subscription charge is to be included in the unit price.

Q. No.	Reference	Query, in brief	Reply of KSRTC
Y-3	Page 23, Section V — Managed MySQL	For high availability a minimum of three nodes is required; request to change the quantity to 3.	The quantity is not altered. See amendment B-18: the quantity denotes managed database deployments, and the unit price is to be inclusive of every node, replica and licence required for the high-availability configuration offered.
Y-4	Page 23, Section V — block volume for boot and application	Request to change the performance to 6 IOPS per GB.	Accepted. See amendment B-5 — not less than 6 IOPS per GB, subject to a minimum of 3,000 IOPS per application volume.
Y-5	Page 23, Section V — block volume for database	Request to change the performance to 6 IOPS per GB.	Accepted. See amendment B-5 — not less than 6 IOPS per GB, subject to a minimum of 5,000 IOPS per database volume.
Y-6	Page 23, Section V — object storage, standard tier	Request to change the indicative quantity to a usage basis.	Not accepted. The quantities in column D are indicative only and are used solely to arrive at a single comparable figure for evaluation (Note 4 to the Bill of Quantity, read with Clause 12 of Section II). Invoicing is in every case on actual consumption at the unit rates quoted. Quantities cannot be left open, as the Financial Bids would then not be comparable.
Y-7	Page 23, Section V — object storage for backup and archive	Request to change the indicative quantity to a usage basis.	Not accepted, for the reasons stated against Y-6.
Y-8	Page 23, Section V — Web Application Firewall	Request to change 'native service' to 'cloud service'.	Accepted. See amendment B-8.
Y-9	Page 23, Section V — disaster recovery replication	Request for the total number of virtual machines, and observation that RPO and RTO depend on the sizing.	The estate as indicatively sized comprises fourteen (14) virtual machines and three (3) managed database deployments. The scope and pricing basis of the disaster recovery lot are now defined by amendment B-10, and the compute at the Disaster Recovery site is billed on actual consumption at the quoted compute rates rather than within the lot.
Y-10	Page 23, Section V — Web Application Firewall	Request for the number of applications requiring WAF protection and the bandwidth of each.	The internet-facing applications to be protected number six (6), being the workloads at serial numbers 1, 2, 3, 4, 6 and 7 of Annexure B, with an aggregate perimeter bandwidth of 300 Mbps. The workload at serial number 5 of Annexure B is device telemetry ingestion and is to be protected by the network firewall and the DDoS service and not by the Web Application Firewall. The Web Application Firewall line item is a monthly lot inclusive of fifty million (50,000,000) requests per month and of unlimited rules and policies.
Y-11	Page 24, Section V — vulnerability scanning	VAPT is required twice a year but the indicative quantity is one per month; clarification sought.	Both are required and they are different exercises. See amendment B-20: the priced line item is one automated operating-system-level scan of the full estate each month; the half-yearly vulnerability assessment and penetration testing under Clause 3.3 of

Q. No.	Reference	Query, in brief	Reply of KSRTC
			Section IV is included in the managed services lot and is not separately priced.
Y-12	Page 24, Section V — scope of vulnerability scanning	Whether the requirement is a network vulnerability assessment covering internal and external security and device-level policy, together with penetration testing.	The monthly line item is an automated assessment at operating system level covering missing patches, packages, open ports and CIS benchmark compliance. The half-yearly exercise is a full vulnerability assessment and penetration test covering internal and external assessment, device-level and security-group policy review and application-level penetration testing, conducted by an agency empanelled with the Indian Computer Emergency Response Team, with the report, remediation plan and evidence of closure furnished to KSRTC.
Y-13	Page 24, Section V — DDoS protection	Whether DDoS protection is always on, with a total bandwidth of 300 Mbps.	Confirmed. Protection shall be always on, and shall be sized to the perimeter bandwidth of 300 Mbps reflected in the load balancer line item. Protection at Layer 7 with customisable rules is additionally required by requirement 23 of Annexure A.
Y-14	Page 24, Section V — bastion service	Request to permit a virtual private network for secure access to private subnets.	Accepted. See amendment B-16 — a bastion service or an equivalent privileged-access service comprising an SSL or IPSec VPN with a hardened jump host, with multi-factor authentication and session recording.
Y-15	Page 24, Section V — managed DNS	Request for the total number of domains.	Five (5) hosted zones, comprising the public zones of the Corporation, the private zone of the virtual network and the zone for the test and staging environment. The line item is a monthly lot inclusive of ten million queries.
Y-16	Page 47, Annexure A, requirement 24 — identity and access management	Request for the total user or device count for an IAM/PAM solution.	Identity and access management is a platform capability under requirement 24 and is not separately priced. The requirement relates to access to the cloud tenancy and not to the end users of the applications hosted in it; end users of the applications are outside the scope of this requirement. Multi-factor authentication is mandatory for every principal holding console or administrative access to the tenancy, whether of KSRTC, of the Contractor or of an application vendor. For sizing, thirty (30) such principals require multi-factor authentication, of whom ten (10) are privileged administrators to be brought under privileged access management, that number including the holders of the root or owner credentials which vest in KSRTC under Clause 2 of Section IV.
Y-17	Page 47, Annexure A, requirement 12 — key management	Whether a managed hardware security module and key management service are required.	See amendment B-7. The requirement is relaxed, and no key management or hardware security module service is to be priced in the Financial Bid. If KSRTC elects to use customer-managed keys,

Q. No.	Reference	Query, in brief	Reply of KSRTC
			the service will be provisioned under Clause 8 of Section IV at list price less the Additional Services Discount.
Y-18	Page 24, Section V — SIEM unit of measurement	Request to price per device per month instead of per GB per month.	Not accepted. See amendment B-21. A single unit of measurement is necessary for the Financial Bids to be comparable on one Total Evaluated Bid Value; a Bidder whose provider prices per device shall convert to the per-GB unit. The retention periods are now specified.
Y-19	Page 24, Section V — managed threat detection	Whether threat detection may be bundled with SIEM on a per-device basis.	The two services may be delivered as one managed offering, but each of the two line items must carry a separate rate in the Bill of Quantity. A Bid that prices the two as a single line, or that quotes Rs. 0 against either, shall be rejected under Clause 5.2 of Section II.
Y-20	Page 28, Section VI / Form 1, item 10 — support location	Request to permit support from locations other than Thiruvananthapuram.	Accepted in part. See amendment B-15 — a support presence anywhere in Kerala, with attendance in person at Transport Bhavan within four hours for a Severity 1 incident. The on-site cloud engineer during migration remains as provided by Clause 3.4 of Section IV.
Y-21	Pages 3 and 40, Section I and Form 6 — EMD or Bid Securing Declaration	Clarification sought whether an EMD of Rs.1,00,000/- is to be furnished or the declaration in Form 6 suffices.	See amendment B-1. The Earnest Money Deposit of Rs.1,00,000/- and the tender document fee are payable online through the e-GP Portal. Form 6 is to be furnished only by a Bidder claiming exemption from the Deposit, together with the valid exemption certificate.
Y-22	Page 46, Annexure A, requirement 10 — IOPS	Request to reduce to 6 IOPS per GB for both storage types.	Accepted, with per-volume minimums. See amendment B-5.
Y-23	Page 46, Annexure A, requirement 11 — dynamic IOPS change	Request to delete the requirement, as a change may require a restart depending on the guest operating system.	Accepted in part. See amendment B-6 — the requirement is retained but a restart in an approved maintenance window is permitted where the guest operating system requires it, and the resulting downtime is excluded from availability.
Y-24	Page 47, Annexure A, requirement 12 — HSM-based encryption for storage	Request to remove the HSM-based encryption requirement.	Accepted in part. See amendment B-7. Encryption at rest by default using AES-256 or an equivalent standard is retained and is not relaxed; the FIPS 140-2 Level 3 hardware security module requirement is relaxed where the Cloud Service Provider does not offer a dedicated HSM service.
Y-25	Page 47, Annexure A, requirement 18 — leased line or direct connect	Request for the sizing of the dedicated leased line or direct connect in Mbps.	Requirement 18 is a capability requirement: the option must be available on the platform. It is not a priced line item in the Bill of Quantity and no bandwidth need be quoted. KSRTC does not propose to take a direct connection at the commencement of the Contract, internal access being over the site-to-cloud

Q. No.	Reference	Query, in brief	Reply of KSRTC
			virtual private network established under Clause 3.4 of Section IV. Should KSRTC elect to take one during the Contract, the indicative requirement is 100 Mbps, and it will be provisioned under Clause 8 of Section IV, the existing link and virtual private network being retained as fallback.
Y-26	Page 47, Annexure A, requirement 20 — native API gateway	Request to remove 'native' as a mandate for the API gateway.	Accepted. See amendment B-8.
K-1	Section IV, Clause 3.1 — high availability of virtual machines	Whether the virtual machines in the Bill of Quantity are already in a high-availability configuration, or whether high availability is to be designed additionally.	The quantities at Section V represent the aggregate compute to be provisioned and are not to be doubled for high availability. The Bidder shall design the distribution of those instances across availability domains and fault domains so as to meet the uptime commitments at requirement 27 of Annexure A and the service level matrix at Clause 6.3 of Section IV. Where additional instances are required at any time, they shall be provisioned under Clause 12 of Section II at the unit rates quoted.
K-2	Section IV, Clause 3.2 — DR topology	Whether disaster recovery is active-active or active-passive.	Active-passive. See amendment B-10.
K-3	Section IV, Clause 3.3 — key management service	Whether a key management service is required, since it is not in the Bill of Quantity, and the number of customer master keys and monthly requests.	See amendment B-7. No key management service is to be priced in the Financial Bid. If KSRTC elects to use customer-managed keys, the service will be provisioned under Clause 8 of Section IV at list price less the Additional Services Discount.
K-4	Section V — scope of the BoQ quantities	Whether the quantities apply to the Data Centre only or include the Disaster Recovery site.	The quantities in column D relate to the Data Centre. The Disaster Recovery site is covered by the disaster recovery replication lot, whose scope is now defined by amendment B-10; compute instantiated at the Disaster Recovery site is billed on actual consumption at the quoted compute rates.
K-5	Section V — managed threat detection quantity	Basis of the quantity of 15 questioned, the schedule showing 14 virtual machines and 3 managed database instances.	The inconsistency is admitted and corrected. See amendment B-11 — the quantity is 17.
K-6	Section V — next-generation firewall and VPN	Confirmation sought of the number of VPN users.	Requirement 18 is a capability requirement: the option must be available on the platform. It is not a priced line item in the Bill of Quantity and no bandwidth need be quoted. KSRTC does not propose to take a direct connection at the commencement of the Contract, internal access being over the site-to-cloud virtual private network established under Clause 3.4 of Section IV. Should KSRTC elect to take one during the Contract, the indicative

Q. No.	Reference	Query, in brief	Reply of KSRTC
			requirement is 100 Mbps, and it will be provisioned under Clause 8 of Section IV, the existing link and virtual private network being retained as fallback.
K-7	Section VI, Clause 2, criterion 4 — experience	Request that work orders relevant to the case, with project details, be accepted.	The requirement is unchanged: copies of the work orders relied upon, with completion certificates or, for ongoing work, a satisfactory-performance certificate up to the quarter preceding publication together with the value of work completed. Commercially sensitive rates within a work order may be masked, provided that the client, the scope, the value and the period remain legible.
A-1	Page 28, Section VI, Clause 2, criterion 2 — certified resources	Request to accept associate-level certifications of any leading hyperscaler where the proposed CSP operates no certification programme, and to accept a self-declaration in place of individual certificates.	Accepted. See amendment B-9. Certifications of Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure or IBM Cloud are acceptable where the proposed Cloud Service Provider does not operate a certification programme, supported by a declaration of that Provider; and the signed statement at Part B of Form 3 suffices, individual certificates not being required with the Bid.
A-2	Technical — current HLD/LLD	Request for the current high-level and low-level design covering application and network flows for the DC and DR environments.	Not furnished at the bid stage. Disclosure of the network and security design of the Corporation at the bid stage is declined on security grounds. The design is to be established through the discovery exercise at Milestones 1 and 2 of Clause 5 of Section IV, and the relevant material will be furnished to the successful Bidder under the Non-Disclosure Agreement in Form 8.
A-3	Technical — application inventory and dependency mapping	Request for the application inventory with application, virtual machine and database dependency mapping.	Annexure B, as amended by B-4, is the inventory furnished at the bid stage. Dependency mapping is a deliverable of the discovery exercise and is to be produced by the Contractor jointly with KSRTC within fifteen (15) working days of the Purchase Order.
A-4	Technical — database inventory	Request for database inventory, version, size, edition, licensing and HA configuration.	The database inventory, with version, edition, size and high-availability configuration, is a deliverable of the discovery exercise at Milestone 1 of Clause 5 of Section IV and will be furnished to the successful Bidder under the Non-Disclosure Agreement in Form 8. Bidders shall price on the basis of the managed MySQL and managed PostgreSQL line items in Section V. Should discovery disclose a workload running any other engine, it shall be migrated either to an equivalent managed service of the Cloud Service Provider or

Q. No.	Reference	Query, in brief	Reply of KSRTC
			to a virtual machine and provisioned under Clause 8 of Section IV, and no claim shall lie against KSRTC on account of the difference. Licences for any proprietary database engine remain the responsibility of KSRTC unless otherwise agreed.
A-5	Technical — database deployment model	Whether databases are to be deployed on virtual machines or as a PaaS service.	As a managed platform service where the engine is MySQL or PostgreSQL — three deployments are priced. Any other engine is to be deployed on a virtual machine.
A-6	Technical — DC and DR regions	Confirmation sought of the proposed DC and DR regions.	The regions are for the Bidder to propose, subject to requirement 2 of Annexure A and to criterion 2 of Clause 1 of Section VI — within India, in different seismic zones, not less than 250 km apart, and each live for not less than two years. The locations offered are to be stated in Form 5.
A-7	Technical — internet-facing applications and public IP addresses	Request for the list of internet-facing applications and the number of public IP addresses.	The list is not published at the bid stage. The number of internet-facing applications is six (6), as stated in the reply at Y-10. Four (4) public static IP addresses are priced in the Bill of Quantity; the applications are fronted by the two load balancers priced in the same schedule, and the four addresses are accordingly the two load balancers, the network address translation gateway and the virtual private network or bastion endpoint.
A-8	Technical — network connectivity	Whether existing connectivity is retained or new connectivity is required, and the MPLS, internet and DC–DR replication bandwidth required.	The existing connectivity of KSRTC at the Chief Office, Transport Bhavan, being a 225 Mbps 1:1 internet leased line provided by Kerala Fibre Optic Network Limited, is retained. The Contractor shall provide the site-to-cloud virtual private network and the DC–DR replication bandwidth, the latter being included in the disaster recovery lot under amendment B-10. No MPLS circuit is required. A dedicated leased line or direct connect, if elected by KSRTC, will be provisioned under Clause 8 of Section IV
A-9	Technical — security services	Whether the security services are to be newly deployed, with throughput and licensing details.	All security services required by Section IV and Annexure A are to be newly deployed on the proposed platform; none is to be carried over. The perimeter is to be sized at 300 Mbps, consistent with the load balancer line item. All licences, subscriptions and tooling are to be included in the rates quoted, no separate charge being payable (Note 10 to the Bill of Quantity).

Q. No.	Reference	Query, in brief	Reply of KSRTC
A-10	Technical — responsibility for OS redeployment and application migration	Confirmation sought that the cloud provider is responsible for infrastructure provisioning and infrastructure-level migration, and the application vendor for application redeployment, code changes, compatibility fixes and testing.	Confirmed, and now recorded in the Tender Document by amendment B-13.
A-11	Technical — DR orchestration tool	Which DR orchestration or DRM tool is currently in use.	None. The Contractor shall propose the replication and orchestration mechanism in the migration and implementation approach note, and its cost is included in the disaster recovery lot.
A-12	Technical — DR requirements	Request for RTO, RPO, uptime, DR strategy and drill frequency.	Recovery Point Objective thirty (30) minutes; Recovery Time Objective four (4) hours; availability as in the service level matrix at Clause 6.3 of Section IV; active-passive for both application and database tiers, as now provided by amendment B-10; drills twice in each year of the Contract.
A-13	Technical — ITSM tool	What ITSM tool is currently in place.	None is prescribed. The Contractor shall provide the ticketing system required by Clause 3.5 of Section IV, generating an acknowledgement identifier on booking and on closure and automatically escalating tickets left open beyond the prescribed timelines, with access for the IT Division of KSRTC.
A-14	Technical — applications to be onboarded on the WAF	Request for the number of internet-facing applications to be onboarded on the Web Application Firewall.	Six (6). See the reply at Y-10, which also identifies the six workloads and explains why the vehicle location and tracking workload is not among them.
A-15	Technical — SIEM log retention	Confirmation sought of the log retention period for the SIEM.	See amendment B-21, which now specifies the online and archival retention periods.
A-16	Technical — MFA, IAM and PAM	Whether MFA is required for administrators or for all users, and the user counts for MFA and PAM.	See the reply at Y-16. Multi-factor authentication is mandatory for every administrative principal; the counts for sizing are stated there.
A-17	Technical — VAPT scope	Request for the number of applications to be penetration tested and confirmation that the scope is limited to assets and applications hosted on the cloud.	Confirmed. The scope is confined to the assets and applications hosted on the cloud under this Contract, being the workloads at Annexure B. See also amendment B-20.
A-18	Technical — DLP, DSPM and CSPM	Whether cloud DLP, network DLP, DSPM and CSPM are in scope, and the database types if so.	Cloud security posture management is in scope: it is a mandatory platform capability under requirement 25 of Annexure A and its operation is included in the managed services lot. Cloud data loss prevention, network data loss prevention and data security posture management are outside the scope of this tender. Should KSRTC require any of them during the Contract, it will be provisioned under Clause 8 of Section IV.
R-1	Representation on Office	Representation that no Category A	The representation has been examined.

Q. No.	Reference	Query, in brief	Reply of KSRTC
	Memorandum F.No.9(3)/2025-EG-II dated 20.03.2026 of MeitY	/ Category B classification of applications and data was recorded before the tender was structured around private MeitY-empanelled Cloud Service Providers, and that the nomination route under paragraph 4(i) of the Office Memorandum is excluded without recorded reasons.	The classification of the applications and data at Annexure B is now recorded in the Tender Document by the new Clause 1A inserted by amendment B-17, and any workload classified as Category A stands excluded from the scope of this Contract until KSRTC directs otherwise. Participation is simultaneously widened by amendment B-17 to entities eligible under the nomination route recognised by paragraph 4(i) of the Office Memorandum, including the National Informatics Centre, State Data Centres and Public Sector Undertakings and entities under the administrative control of the Ministry of Electronics and Information Technology that have onboarded a MeitY-empanelled Cloud Service Provider through the Government e-Marketplace or through an open request for proposal. The extension of the last date for the submission of Bids by fourteen (14) days affords such entities adequate opportunity to participate.

Part D — General

1. No query other than those answered at Part C has been received within the time allowed by the Bid Data Sheet, and no further pre-bid meeting will be held.

2. The relaxations granted by this Corrigendum are granted uniformly to all Bidders and do not confer any advantage on the Bidder at whose instance a query was raised. No relaxation has been granted in respect of the location of the Data Centre and the Disaster Recovery Centre within India, the localisation of data, the ownership of the tenancy by KSRTC, the Recovery Point and Recovery Time Objectives, the service level regime, or the exit management obligations.

3. Nothing in this Corrigendum shall be construed as a warranty by KSRTC as to the accuracy, adequacy or completeness of any figure furnished for the purpose of sizing. Bidders shall conduct their own due diligence, and Clause 6 of Section I continues to apply.

4. The rights reserved to KSRTC by Clause 6 of Section I, including the right to reject any or all Bids and to cancel the Tender Process at any stage, are unaffected by this Corrigendum.

Deputy General Manager (I T)
for and on behalf of the Chairman and Managing Director
Kerala State Road Transport Corporation