ANNEX -SLA

SERVICE LEVEL AGREEMENTS (SLAs)

For Inclusion in Section IIV – Functional Requirements Schedule (FRS)

Metro Bus Digital Platform (MBDP)

Procurement No: LMT/DM/PRO/2026/001/R00

Lanka Metro Transit (Pvt) Ltd

This schedule defines the Service Level Agreements applicable to the Metro Bus Digital Platform. Because the platform is deployed in phases, SLA obligations commence independently for each phase upon its respective Phase Acceptance and remain in effect throughout the mandatory first-year maintenance period and the subsequent revenue-sharing contract period for that phase. These SLAs are aligned with FRS v2.0 Part E (Non-Functional Requirements Traceability) and supersede any conflicting statements in earlier project documents.

1. SCOPE AND APPLICABILITY

These SLAs apply from the date of final system acceptance (completion of Stabilization Period) and remain in effect throughout:

1. The mandatory first-year maintenance period (Year 1 post-acceptance).
2. The subsequent revenue-sharing contract period (Years 2–5).

During the development and phased deployment period (Phases 1–5), separate acceptance criteria defined in FRS Part E govern system performance. The SLAs in this schedule take full effect only after final system acceptance.

The Vendor shall be responsible for maintaining all software components of the MBDP platform, including but not limited to server-side applications, APIs, databases, mobile applications, web applications, on-bus software, bus stop display software(only if necessary), and all integration interfaces. The Purchaser is responsible for the underlying infrastructure (Lanka Government Cloud hosting, network connectivity, and hardware maintenance), though the Vendor must promptly report any infrastructure issues that affect SLA compliance.

2. SYSTEM AVAILABILITY AND UPTIME

System availability is measured as the percentage of time the system is operational and accessible to users during the measurement period, excluding Scheduled Maintenance Windows. A tiered uptime model applies, reflecting the operational criticality of each component group.

2.1. Availability Tiers

Tier	Components	Uptime Target	Notes
Tier 1 Embedded Systems	On-bus systems (tapping machines, GPS, HMI, CCTV software), bus stop display systems	**99.9%**	Highest reliability. Measured per device. Offline operation must function when connectivity is lost. Maximum allowable downtime: ~40 minutes/month per device.
Tier 2 Core Platform	Backend APIs, databases, payment processing, authentication, fare calculation engine, and real-time GPS data processing	**99.5%**	Contractual SLA. Measured end-to-end. Maximum allowable downtime: ~3.6 hours/month. This is the primary tier for SLA penalty calculations.
Tier 3 Non-Critical Services	Reports, analytics dashboards, custom report builder, admin tools, advertising management, data warehouse/ETL	**99.0%**	Degraded mode acceptable. Delayed availability does not constitute a Critical incident. Maximum allowable downtime: ~7.3 hours/month.

2.2. Availability Calculation

Availability % = ((Total Minutes – Scheduled Maintenance – Unplanned Downtime) / (Total Minutes – Scheduled Maintenance)) × 100

The measurement period is one calendar month. Availability is calculated separately for each tier. For Tier 1 (embedded systems), availability is the fleet-wide average across all active devices.

2.3. Scheduled Maintenance Windows

Parameter	Requirement
Standard Maintenance Window	Saturday and Sunday, 01:00 AM – 05:00 AM Sri Lanka Time (4 hours)
Extended Maintenance Window	By prior written approval from the Purchaser, with a minimum of 72 hours' advance notice. Maximum once per month.
Emergency Maintenance	Permitted at any time for Critical severity issues. Vendor must notify Purchaser within 30 minutes of initiating emergency maintenance and provide a post-maintenance report within 24 hours.
Maximum Monthly Maintenance Hours	16 hours total (including both standard windows). Exceeding this without prior approval constitutes unplanned downtime for SLA purposes.
Advance Notice for Scheduled Maintenance	Minimum 48 hours advance written notification to the designated Purchaser contact, specifying scope, expected duration, and affected services.

3. INCIDENT CLASSIFICATION AND RESPONSE

All incidents shall be classified by severity level based on their operational impact. The classification determines the required response and resolution times.

3.1. Severity Classification

Severity	Definition	Response Time	Resolution Time
Critical	System is down, or payment processing has failed – bus operations cannot proceed. Examples: fare collection system-wide failure, GPS data completely unavailable to OCC, GovPay down, authentication service down, database corruption affecting live operations.	**1 hour**	**4 hours**
High	Major feature is unavailable, but a workaround exists – operations can continue in degraded mode. Examples: real-time tracking delayed beyond 60 seconds, one route's scheduling system down, reporting module unavailable, mobile app login intermittent for a subset of users.	**4 hours**	**24 hours**
Medium	Minor bug affecting a limited number of users – no operational impact. Examples: a single report generating incorrect totals, a non-critical UI element displaying incorrectly, one bus stop display showing stale data, a minor translation error.	**1 business day**	**5 business days**

Low	Cosmetic defect or documentation issue with no functional impact. Examples: font inconsistency, tooltip text error, user guide correction needed, minor alignment issue on a non-critical screen.	**3 business days**	**15 business days**

3.2. Response and Resolution Definitions

Response Time is the elapsed time from when an incident is reported through the agreed channel (helpdesk, monitoring alert, or email) to when the Vendor acknowledges the incident in writing and assigns qualified technical personnel to begin investigation.

Resolution Time is the elapsed time from incident reporting to when the system is restored to normal operation (for Critical/High) or a permanent or acceptable temporary fix is deployed (for Medium/Low). A temporary workaround accepted by the Purchaser pauses the resolution clock for Medium and Low severity only.

3.3. Incident Support Hours

Severity	Support Availability
Critical	24 hours × 7 days (including public holidays). The Vendor must maintain an on-call technical team reachable within 15 minutes at all times.
High	24 hours × 7 days for initial response. Resolution work may continue during business hours unless the Purchaser requests extended hours.
Medium / Low	Business hours: Monday to Friday, 8:30 AM – 5:00 PM Sri Lanka Time, excluding gazetted public holidays.

3.4. Escalation Procedure

Escalation Level	Trigger	Vendor Action	Purchaser Contact
Level 1 Technical	Incident reported	The assigned engineer begins the investigation	IT Helpdesk Coordinator
Level 2 Team Lead	Response time exceeded, or Critical incident not resolved within 2 hours	Senior technical lead assumes ownership; additional resources mobilized	IT Manager
Level 3 Management	Resolution time exceeded, or Critical incident not resolved within 4 hours	Vendor's Project Director personally engages; war room established	IT Manager Assistance
Level 4 Executive	Critical incident exceeds 8 hours unresolved	Vendor CEO / MD is notified and provides a written action plan within 2 hours	LMT CEO / Chairman

4. PERFORMANCE SLAs

The following performance targets apply at all times during operational hours. These are derived from FRS v2.0 Part E and are contractually binding.

4.1. Transaction and Processing Performance

Metric	Target	Measurement Method	Applicable Modules
Fare tap-in/tap-out transaction processing	**< 2 seconds end-to-end**	Transaction log timestamps	On-Bus, Payment
GPS position update frequency	**Every 10 seconds**	GPS data feed monitoring	On-Bus, Fleet Mgmt
GPS data to passenger-visible information	**< 10 seconds**	End-to-end latency test	Passenger App, OCC
GTFS-RT feed latency from position change	**< 30 seconds**	Feed timestamp comparison	Public Info Services
Fare transaction to general ledger posting	**Within 1 hour**	GL posting timestamp	Finance, On-Bus
Customer complaint routing to operations	**Within 15 minutes**	Workflow timestamp	Passenger, OCC
Driver schedule sync to payroll	**Within 1 hour**	Sync log comparison	HR, Fleet Mgmt
Work order parts consumption to inventory	**Real-time**	Stock level audit	Maintenance, Stores
Web page load time (95th percentile)	**< 3 seconds**	Synthetic monitoring	All web modules
Mobile app screen load time (95th percentile)	**< 2 seconds**	App performance monitoring	All mobile modules
API response time (95th percentile)	**< 1 second**	API gateway logs	All API endpoints

4.2. Throughput and Capacity

Capacity Metric	Minimum Target	Notes
Daily fare transactions (125 buses)	**30,000 transactions/day**	Average 300 transactions per bus per day
Peak hour throughput	**3× average hourly rate sustained for 2 hours**	Must not degrade response times
Concurrent passenger app users	**500 simultaneous sessions**	Without performance degradation
Staff mobile app	**125 simultaneous sessions**	Bus operator assistance and all back-office staff
Concurrent web admin users	**50 simultaneous sessions**	Back-office staff
Daily batch processing (ETL/reporting)	**Completed within 4 hours**	Must complete before 06:00 AM daily

5. DATA INTEGRITY AND BACKUP SLAs

Requirement	SLA Target
Database backup frequency	Full backup: daily. Incremental backup: every 6 hours. Transaction log backup: every 1 hour.
Backup verification	Automated restore test of the most recent backup at least once per week. Written confirmation provided to the Purchaser monthly.
Recovery Point Objective (RPO)	Maximum 1 hour of data loss for Tier 2 (Core Platform) services. Maximum 6 hours for Tier 3 services.
Recovery Time Objective (RTO)	4 hours for Tier 2 services. 8 hours for Tier 3 services. Tier 1 embedded systems: offline operation continues; sync within 30 minutes of connectivity restoration.
Fare transaction data integrity	Zero data loss for completed fare transactions. Every tap-in/tap-out must be reconcilable in the financial ledger. Daily reconciliation variance must not exceed 0.1%.
Disaster recovery test	Full disaster recovery simulation at least once every 6 months. The Purchaser shall be notified and invited to observe. Written report provided within 5 business days.

6. SECURITY SLAs

Requirement	SLA Target
Critical security patch deployment	Within 24 hours of vendor notification for zero-day vulnerabilities affecting production systems. Within 72 hours for other critical patches.
Vulnerability scanning	Automated vulnerability scans: weekly. Penetration testing: at least once every 6 months or after any major release. Reports shared with the Purchaser within 5 business days.
Security incident response	Classified as Critical severity. Initial containment within 1 hour. Full investigation report to the Purchaser within 48 hours. Government SOC notified within 2 hours per the SOC integration requirements.
SL-CERT compliance	Maintain valid SL-CERT security clearance at all times. Any change in clearance status must be reported to the Purchaser immediately.
SSL/TLS certificate management	Certificates renewed at least 30 days before expiry. No expired certificates in production at any time.
Access audit logs	All administrative access logged. Logs retained for a minimum 12 months. Monthly access review report provided to the Purchaser.

7. SLA REPORTING AND MONITORING

7.1. Monthly SLA Report

The Vendor shall deliver a written monthly SLA performance report to the Purchaser by the 5th business day of the following month. The report shall include:

1. System availability percentage for each tier, with a detailed downtime log.
2. Total number of incidents by severity level, with response and resolution times for each.
3. Number of SLA breaches by category, with root cause analysis for each breach.
4. Performance metrics dashboard showing all targets from Clause 4 versus actual measurements.
5. Backup and recovery test results.
6. Security scan summaries and patch deployment status.
7. Scheduled and unscheduled maintenance log with duration and affected services.
8. Trending analysis comparing the current month to the previous three months.

7.2. Real-Time Monitoring Dashboard

The Vendor shall provide the Purchaser with access to a real-time monitoring dashboard that displays, at a minimum: system availability status for each tier, active incident count by severity, current API response times, GPS data feed health, payment gateway status, and active user counts.

7.3. Quarterly Service Review

A formal quarterly service review meeting shall be held between the Vendor and Purchaser to review overall SLA performance, discuss improvement opportunities, plan upcoming maintenance activities, and address any systemic issues. The Vendor shall prepare and distribute the meeting agenda and materials at least 5 business days in advance.

8. SLA CREDITS AND PENALTIES

Failure to meet SLA targets shall result in service credits applied against the Vendor's monthly maintenance or revenue-sharing payments. These credits are not penalties but compensation for diminished service quality.

8.1. Availability Credits

Tier	Target	Actual Availability	Monthly Service Credit
Tier 2 – Core Platform	99.5%	99.0% – 99.49%	5% of monthly payment
		98.0% – 98.99%	10% of monthly payment
		95.0% – 97.99%	20% of monthly payment
		Below 95.0%	30% of monthly payment + Purchaser may issue a cure notice

> ***Note:*** *If Tier 2 availability falls below 95% for two consecutive months, the Purchaser reserves the right to terminate the contract for cause after providing a 30-day cure period.*

8.2. Incident Resolution Credits

Severity	Resolution Target	Actual Resolution	Credit per Incident
Critical	4 hours	4–8 hours	LKR 100,000 per incident
		> 8 hours	LKR 250,000 per incident
High	24 hours	24–48 hours	LKR 50,000 per incident
		> 48 hours	LKR 100,000 per incident

8.3. Monthly Credit Cap

The total service credits in any single calendar month shall not exceed 30% of the monthly payment amount for that month. This cap does not limit the Purchaser's right to terminate for persistent poor performance or to claim damages for losses beyond the credit cap under the general conditions of contract.

8.4. Chronic Failure

If the Vendor fails to meet Tier 2 availability targets for three or more months in any rolling twelve-month period, or if the cumulative service credits exceed 20% of the annual maintenance fee, this shall constitute a material breach. The Purchaser may issue a formal cure notice requiring the Vendor to submit a remediation plan within 10 business days. Failure to remedy within 60 days of the cure notice entitles the Purchaser to terminate the contract.

9. SLA EXCLUSIONS

The following events are excluded from SLA calculations, provided the Vendor can demonstrate that the downtime or performance degradation was caused solely by the excluded event:

1. Scheduled maintenance conducted within approved maintenance windows as per Clause 2.3.
2. Force majeure events (natural disasters, civil unrest, government-mandated shutdowns) as defined in the General Conditions of Contract.
3. Infrastructure failures within the Lanka Government Cloud (LGC) or third-party network providers that are outside the Vendor's control, provided the Vendor notifies the Purchaser within 30 minutes and provides evidence of the third-party cause.
4. Failures caused by the Purchaser's unauthorized modifications to system configurations, data, or infrastructure.
5. GovPay/LankaPay or SL-UDI outages that are confirmed as third-party service failures by the respective government agency.
6. Denial-of-service attacks, provided the Vendor has maintained agreed security measures and responds per the security SLA in Clause 6.

> ***Note:*** *The burden of proof for exclusions rests with the Vendor. All exclusion claims must be submitted in writing within 5 business days of the event, with supporting evidence. The Purchaser's determination of whether an exclusion applies is final.*

10. CONTINUOUS IMPROVEMENT

The Vendor shall implement a continuous improvement programme throughout the contract period, including:

1. Trend analysis of incidents to identify and address recurring issues proactively.
2. Quarterly capacity planning reviews to ensure the platform can handle growing usage.
3. Annual review of SLA targets with the Purchaser, with the possibility of tightening targets based on system maturity and performance history.
4. Knowledge base maintenance, documenting all resolved incidents and their solutions.
5. Post-incident reviews for all Critical and High severity incidents, with root cause analysis and preventive action plans shared with the Purchaser within 5 business days.

11. SLA DURING STABILIZATION PERIOD

During the four-week Stabilization Period following Phase 5 completion, relaxed SLA targets apply as the system undergoes final integration testing and load testing:

Parameter	Stabilization Target	Post-Acceptance Target
Tier 2 Availability	99.0%	**99.5%**
Critical Response Time	2 hours	**1 hour**
Critical Resolution Time	8 hours	**4 hours**
SLA Credits	Not applicable	**Fully applicable**

The Stabilization Period ends when the Purchaser issues a Final System Acceptance Certificate. If acceptance is delayed due to unresolved Critical defects, the stabilization SLA targets continue until acceptance is achieved, but the Vendor is not entitled to claim additional payments for the extended stabilization.

END OF SERVICE LEVEL AGREEMENTS