Ujjain Smart City Limited

Request for Proposal for

Selection of System Integrator (SI) for

Establishment and O&M of Integrated Command & Control Centre (ICCC) for Simhastha Kumbh Mela 2028

Volume – 3: DRAFT CONTRACT AGREEMENT & SERVICE LEVEL AGREEMENT (SLA)

NIT No. USCL/430

Tender ID: 2026_UAD_508730_1 **Ujjain Date: 20/05/2026**

……..

Ujjain Smart City Limited
Simhastha Mela Office, Kothi Road,
Ujjain, Madhya Pradesh – 456010

Establishment and O&M of Integrated Command & Control Centre (ICCC) for Simhastha Kumbh Mela 2028

VOLUMES STRUCTURE OF RFP DOCUMENTS

Volume	Contents
Volume-I	Instructions to Bidders and Bid Process Management
Volume-II	Scope of Work & Technical Specifications
Volume-III	Draft Contract Agreement & SLA
Volume-IV	Financial Bid / BOQ

Volume – 3: DRAFT CONTRACT AGREEMENT (DCA) & SERVICE LEVEL AGREEMENT (SLA)

TABLE OF CONTENTS

Section	Description
Preamble	Contract Introduction
Part A	General Conditions of Contract (GCC)
Part B	Special Conditions of Contract (SCC)
Part C	Service Levels & SLA Framework
Part D	Schedules & Annexures

PREAMBLE

This Master Service Agreement ("Agreement") is executed on this ___ day of _____ 2026 at Ujjain, Madhya Pradesh.

BETWEEN

Ujjain Smart City Limited (USCL), a company incorporated under the Companies Act and acting through its Chief Executive Officer, having its office at Simhastha Mela Office, Kothi Road, Ujjain, Madhya Pradesh – 456010 (hereinafter referred to as the "Authority" or "USCL", which expression shall, unless repugnant to the context or meaning thereof, include its successors, administrators and permitted assigns);

AND

M/s _____, a company incorporated under the provisions of the Companies Act and having its registered office at _____ (hereinafter referred to as the "System Integrator" or "SI", which expression shall unless repugnant to the context or meaning thereof include its successors, administrators, legal representatives and permitted assigns).

The Authority and SI are individually referred to as a "Party" and collectively as the "Parties".

WHEREAS, the Authority intends to establish a highly scalable, secure, resilient, AI-enabled and integrated enterprise-grade Integrated Command & Control Centre (ICCC) ecosystem for Simhastha Kumbh Mela 2028 for enabling unified surveillance, crowd management, emergency response coordination, integrated public safety operations, traffic and mobility management, decision intelligence, GIS and Digital Twin enabled situational awareness, disaster response management, cyber monitoring and real-time governance.

WHEREAS, the Project is of strategic national and public importance involving management of extremely large pilgrim footfall, public order, disaster management, emergency response, traffic management, public health coordination, and critical urban and event infrastructure.

WHEREAS, the Authority has selected the SI through a competitive bidding process for undertaking design, engineering, supply, installation, integration, testing, commissioning, operations and maintenance of permanent and temporary/rental ICCC infrastructure under a hybrid deployment model.

NOW THEREFORE, in consideration of mutual covenants and obligations contained herein, the Parties hereby agree as follows:

Section	**Description**
Part A	General Conditions of Contract (GCC)
Part B	Special Conditions of Contract (SCC)
Part C	Service Levels & SLA Framework
Part D	Schedules & Annexures

PART A – GENERAL CONDITIONS OF CONTRACT (GCC)

1. DEFINITIONS AND INTERPRETATION

Unless the context otherwise requires, the following terms shall have the meanings assigned below:

1.1 Definitions

"Acceptance Test"

Means Factory Acceptance Test (FAT), Site Acceptance Test (SAT), User Acceptance Test (UAT), integration testing, failover testing, cybersecurity testing, stress testing, load testing, mock drills, evacuation simulation, crowd surge simulation, redundancy validation, interoperability validation and all other tests required under the Contract.

"AI Analytics Engine"

Means the AI/ML-based software platform deployed under the Project for people counting, crowd density estimation, crowd surge prediction, abnormal behavior detection, object detection, intrusion detection, queue analytics, traffic analytics, ANPR analytics, heatmaps, predictive intelligence, event detection, alert generation and operational decision support.

"Appointed Date"

Means the date communicated by the Authority to the SI for commencement of obligations under the Contract.

"Authority"

Means Ujjain Smart City Limited (USCL) and includes Simhastha Mela Authority and any agency authorized by USCL.

"Business Continuity Plan (BCP)"

Means the comprehensive continuity framework prepared by the SI covering uninterrupted operations during infrastructure failure, cyber incidents, crowd emergencies, natural disasters, connectivity disruptions, utility failures or any event affecting ICCC operations.

"Critical Event Day"

Means major snan days, royal procession days, peak crowd days, emergency periods or any day declared critical by the Authority.

"Cyber Incident"

Means any ransomware attack, malware attack, phishing incident, unauthorized access, credential compromise, data breach, denial-of-service attack, cyber intrusion, malicious activity or cybersecurity compromise.

"Digital Twin Platform"

Means the integrated GIS-enabled 2D/3D visualization and simulation platform comprising live telemetry integration, AI analytics integration, predictive simulation, traffic simulation, crowd flow simulation, infrastructure visualization, incident intelligence and operational decision support.

"Disaster Recovery (DR)"

Means the alternate recovery infrastructure, systems, applications, databases, storage, communication links and operational processes enabling restoration of ICCC operations within prescribed Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

"Event Readiness Certificate"

Means the certificate issued by the Authority after successful completion of all testing, mock drills, simulations, failover validations and operational readiness verification.

"Force Majeure"

Means an event beyond the reasonable control of the affected Party and includes natural disasters, war, riots, epidemic, acts of Government and large-scale civil disturbances.

"Go-Live"

Means commencement of successful live operations of the respective Project component after acceptance by the Authority.

"ICCC"

Means the Integrated Command and Control Centre established under the Project.

"Major Snan Day"

Means designated peak bathing dates notified by the Authority.

"O&M"

Means operations, maintenance, support, monitoring, incident management, preventive maintenance, corrective maintenance and lifecycle support.

"Peak Load Condition"

Means operational conditions where crowd density, video streams, analytics load, network utilization or incident volume exceeds thresholds prescribed by the Authority.

"Permanent Infrastructure"

Means all CAPEX-based infrastructure procured and permanently installed under the Project.

"Rental Infrastructure"

Means temporary/event-based infrastructure deployed on rental basis for Simhastha operations.

"Service Levels" or "SLA"

Means measurable service obligations specified under this Agreement.

"Viewing Centre"

Means decentralized monitoring facility integrated with ICCC for surveillance and operational management.

"War Room"

Means dedicated operational emergency coordination facility activated during critical event periods.

"Works"

Means all activities required for survey, design, supply, installation, integration, testing, commissioning, operations and maintenance of the ICCC ecosystem.

1.2 Interpretation

1. In case of inconsistency, the following order of precedence shall apply:
   a. Corrigenda/Addenda;
   b. Contract Agreement;
   c. Volume III;
   d. Volume II;
   e. Volume I;
   f. Approved Clarifications;
   g. Bid Submission.
2. Words importing singular shall include plural and vice versa.
3. Headings are for convenience only.
4. Interpretation favoring operational continuity, public safety, cybersecurity and uninterrupted ICCC functioning shall prevail.
5. References to laws shall include amendments, re-enactments and statutory modifications.

2. SCOPE OF WORK

2.1 General Scope

The SI shall undertake complete end-to-end design, engineering, procurement, supply, installation, integration, testing, commissioning, operations and maintenance of the ICCC ecosystem for Simhastha Kumbh Mela 2028.

2.2 Hybrid Deployment Model

The Project shall comprise:

A. Permanent Infrastructure

- CAPEX-based deployment;
- Permanent ICCC systems;
- Data Centre infrastructure;
- OFC backbone;
- enterprise software platforms;
- cybersecurity infrastructure;
- permanent surveillance systems;
- 60 months comprehensive warranty and O&M.

B. Temporary / Rental Infrastructure

- Event-specific surveillance systems;

- temporary command centres;
- temporary viewing centres;
- portable field systems;
- temporary communication systems;
- temporary analytics and crowd management systems;
- approximately 9 months deployment and support.

2.3 Broad Components

The Project may include, but shall not be limited to:

- Fixed cameras;
- PTZ cameras;
- Thermal cameras;
- Panoramic cameras;
- Body worn cameras;
- Dash cameras;
- Drone integration;
- Water surveillance systems;
- Video Management System (VMS);
- AI analytics platform;
- Digital Twin platform;
- GIS integration;
- Incident management system;
- ICCC infrastructure;
- Viewing centres;
- War-room infrastructure;
- OFC network;
- Wi-Fi and communication systems;
- Cybersecurity systems;
- SOC/SIEM integration;
- DC/DR infrastructure;
- Public announcement integration;
- Emergency response integration.

2.4 Detailed Services

The SI shall provide:

- Detailed survey and site assessment;
- Detailed engineering and architecture design;
- Procurement and supply;
- Installation and commissioning;
- Integration with existing and third-party systems;
- Cybersecurity implementation;
- Cloud operations where applicable;
- AI tuning and analytics optimization;
- Asset tagging and inventory management;
- Training and capacity building;
- Operational staffing;
- Preventive and corrective maintenance;
- Incident response and escalation management;
- Disaster recovery management;
- Event readiness management.

2.5 Multi-Agency Integration

The SI shall integrate systems with:

- Police Department;
- Mela Authority;
- Existing Smart City ICCC;
- Fire Services;
- Health Department;
- Transport Department;
- Disaster Management Authorities;
- Emergency Response Agencies;
- Municipal Authorities.

2.6 Scalability

The architecture shall support future expansion without major redesign including:

- Additional cameras;
- Additional viewing centres;
- Additional analytics modules;

- Future event integration;
- IoT devices;
- Additional GIS layers;
- Cloud expansion.

3. CONDITIONS PRECEDENT

The SI shall fulfil the following conditions prior to Appointed Date:

- Submission of Performance Bank Guarantee;
- Submission of OEM authorizations;
- Submission of detailed project plan;
- Submission of manpower deployment plan;
- Submission of cybersecurity architecture;
- Submission of DR and BCP plans;
- Submission of incident response plan;
- Submission of escalation matrix;
- Submission of insurance policies;
- Submission of statutory approvals;
- Submission of spare inventory plan;
- Submission of peak snan operational plan.

Failure to comply may constitute material breach.

4. COMMENCEMENT AND PROGRESS

The SI shall commence work immediately upon issuance of Letter of Acceptance or Appointed Date.

The SI shall:

- Mobilize adequate manpower and equipment;
- Deploy multiple implementation teams where required;
- Work in multiple shifts including night shifts if required;
- Ensure milestone achievement within timelines;
- Deploy additional resources without additional cost where delays are attributable to SI.

The Authority may direct acceleration of work in public interest.

5. STANDARDS OF PERFORMANCE

The SI shall perform the services with due diligence, efficiency and in accordance with Good Industry Practices.

Mandatory compliance standards shall include:

Standard	Applicability
ISO 27001	Information Security
ISO 22301	Business Continuity
CERT-In Guidelines	Cybersecurity
ONVIF	Interoperability
MeitY Cloud Guidelines	Cloud Infrastructure
STQC	Applicable systems
NCIIPC Guidelines	Critical Infrastructure
Applicable BIS Standards	Hardware systems

The SI shall ensure:

- Enterprise-grade resiliency;
- High availability architecture;
- No single point of failure;
- Cybersecurity hardening;
- Audit readiness;
- Event readiness.

6. APPROVALS AND CONSENTS

The SI shall obtain all applicable approvals including:

- Road cutting permissions;
- OFC permissions;
- Drone/UAV permissions;
- RF spectrum permissions;
- Telecom permissions;
- Municipal permissions;
- Electrical approvals;
- Equipment certifications;
- Cloud compliance approvals.

The Authority shall facilitate coordination support.

7. OBLIGATIONS OF SYSTEM INTEGRATOR

7.1 General Obligations

The SI shall:

- Ensure complete system integration;
- Ensure interoperability across platforms;

- Provide scalable architecture;
- Maintain operational readiness;
- Ensure uninterrupted services.

7.2 Total System Responsibility

The SI shall remain solely responsible for:

- System functionality;
- Interoperability;
- Uptime;
- Cybersecurity;
- OEM coordination;
- SLA compliance;
- Third-party integration.

Subcontracting shall not dilute SI responsibilities.

7.3 Manpower Obligations

The System Integrator (SI) shall deploy qualified, experienced, competent, and adequately trained personnel for implementation, integration, operations, maintenance, cybersecurity management, AI analytics operations, Digital Twin operations, network management, ICCC operations, and field support services under the Project.

The personnel deployed by the SI shall possess minimum educational qualifications, certifications, and relevant experience as specified in the RFP Volume 2 and approved by the Authority.

The SI shall ensure continuity of key personnel during critical implementation stages, trial runs, major snan days, and high-footfall operational periods.

The Authority reserves the right to seek replacement of any personnel found unsuitable, underperforming, lacking required qualifications, involved in misconduct, or detrimental to Project operations.

The SI shall replace such personnel within timelines specified by the Authority without any additional cost implication to the Authority. All personnel shall undergo police verification where required.

Deployment of minimum manpower shall not limit the SI's responsibility to deploy additional manpower necessary for successful, uninterrupted, and SLA-compliant operations of the ICCC ecosystem.

7.4 Event Readiness Obligations

The SI shall:

- Conduct mock drills;
- Conduct crowd simulations;
- Conduct evacuation simulations;

- Conduct failover testing;
- Maintain standby equipment;
- Maintain emergency response teams;
- Deploy enhanced staffing during peak periods.

7.5 Major Snan Day Obligations

During Major Snan Days, the SI shall ensure:

- 24×7 operations;
- Dedicated war-room operations;
- Zero planned downtime;
- Mobile maintenance teams;
- Emergency escalation support;
- OEM onsite support;
- Standby power and communication systems.

7.6 Operational Continuity

The SI shall ensure:

- Redundant connectivity;
- Redundant storage;
- DR readiness;
- Alternate routing;
- Backup power;
- Failover capability.

8. OBLIGATIONS OF AUTHORITY

The Authority shall:

- Facilitate interdepartmental coordination;
- Provide access permissions;
- Facilitate site access;
- Review deliverables;
- Release payments subject to compliance;
- Facilitate statutory coordination where feasible.
- Subject to Contract provisions, the Authority shall reimburse eligible recurring electricity consumption charges for approved project infrastructure as per certified actuals.

9. PROJECT GOVERNANCE

9.1 Governance Structure

The Authority may constitute:

- Apex Committee;
- Steering Committee;
- Technical Committee;
- Operations Committee;
- Cybersecurity Committee;
- Crisis Management Committee.

9.2 Project Management Office

The SI shall establish a dedicated Project Management Office (PMO) at Ujjain.

9.3 Review Meetings

Mandatory review meetings shall include:

- Daily readiness reviews;
- Weekly project reviews;
- Monthly governance reviews;
- Cybersecurity reviews;
- Critical event reviews.

10. PROJECT PLAN AND REPORTING

The SI shall submit:

- Master Project Plan;
- Deployment Schedule;
- Risk Register;
- Resource Deployment Plan;
- Escalation Matrix;
- Testing Plan;
- Recovery Plan;
- Cybersecurity Compliance Reports.

Indicative reporting obligations:

Report	Frequency
Daily Readiness Report	Daily
Incident Report	Real-Time
Cybersecurity Report	Weekly
Asset Health Report	Weekly

AI Accuracy Report	Weekly
Failover Status Report	Monthly
Crowd Analytics Report	Hourly during peak periods

11. IMPLEMENTATION SCHEDULE

Implementation timelines shall be as specified in Volume-II.

The Authority may:

- Direct phased deployment;
- Direct partial operationalization;
- Revise deployment priorities;
- Accelerate implementation in public interest.

Delays attributable to SI shall attract:

- Liquidated Damages;
- SLA deductions;
- Risk-based recoveries.

12. TESTING, COMMISSIONING AND ACCEPTANCE

12.1 Testing Requirements

The SI shall conduct:

- FAT;
- SAT;
- UAT;
- Integration testing;
- Failover testing;
- Cybersecurity testing;
- VAPT;
- Stress testing;
- Peak load testing;
- Mock drills;
- Evacuation simulation;
- Crowd surge simulation;
- DR drills.

12.2 Mandatory Simulations

Simulation	**Mandatory**

Crowd Surge	Yes
Evacuation	Yes
Network Outage	Yes
Cyber Attack	Yes
ICCC Failover	Yes
Camera Overload	Yes
AI Overload	Yes

12.3 Go-Live

No component shall be declared Go-Live without written approval of the Authority.

12.4 Event Readiness Certification

Event Readiness Certificate shall be mandatory before commencement of live event operations.

13. PAYMENT TERMS

13.1 Payment Categories

Payments shall comprise:

- CAPEX payments;
- Rental infrastructure deployment payments;
- O&M payments;
- SLA-linked payments;
- Training payments;
- Integration milestone payments.

13.2 CAPEX Payment Structure

SNo.	Milestone	Payment (%)
1	Submission & Approval of Detailed Project Plan, Detailed Engineering Design, Architecture, Implementation Plan, Cybersecurity Plan, DR/BCP Plan	5%
2	Supply / Delivery of Hardware, Software, Licenses & Major Equipment at Approved Sites / Stores	25%
3	Installation of Field Infrastructure, ICCC Infrastructure, OFC Network, Cameras, DC/DR, Cybersecurity Systems etc.	20%
4	Integration of all Subsystems including VMS, AI Analytics, Digital Twin, GIS, Third-Party Integrations, Communication Systems etc.	15%
5	Successful Completion of FAT, SAT, UAT, Cybersecurity Testing, VAPT, Failover Testing, Simulation Testing & Trial Runs	10%
6	Go-Live of ICCC Ecosystem and Issuance of Event Readiness Certificate	10%

7	Successful Completion of Simhastha Major Operations / Major Snan Period without Critical SLA Breach	10%
8	Final Acceptance & Submission of As-Built Drawings, Documentation, Asset Register, Knowledge Transfer & Closure Compliance	5%
Total		100%

13.3 Rental Infrastructure Payments

SNo.	Milestone	Payment (%)
1	Mobilization & Deployment of Temporary/Rental Infrastructure	25%
2	Successful Installation & Integration Certification	25%
3	Event Operational Readiness & Trial Run Certification	20%
4	Successful Simhastha Operations including Major Snan Days	20%
5	Decommissioning, Site Restoration & Final Clearance	10%
Total		100%

13.4 O&M Payments

O&M payments shall be released quarterly or monthly subject to SLA compliance.

13.4.1 Permanent Infrastructure O&M (60 Months)

Component	Suggested Payment Mode
Preventive & Corrective Maintenance	Quarterly
Helpdesk & Manpower	Monthly
Cybersecurity Monitoring	Quarterly
Software Support & Upgrades	Quarterly
Spare Support	Quarterly

13.4.2 Temporary Infrastructure O&M (9 Months)

Component	Suggested Payment Mode
Field Operations Support	Monthly
Temporary Network Support	Monthly
Temporary ICCC Operations	Monthly
Event Staffing	Monthly
SLA-linked Retention	15% holdback

13.4.3 Electricity Charges & Utility Reimbursement

The System Integrator (SI) shall be responsible for obtaining, coordinating, maintaining, and operating all temporary and permanent electricity connections required for implementation, commissioning, operations, and maintenance of the Project infrastructure, including but not limited

to ICCC facilities, war rooms, viewing centres, field devices, surveillance systems, communication systems, network infrastructure, poles, switches, and associated project components.

The SI shall initially pay all electricity-related charges including electricity consumption charges, meter charges, temporary connection charges, demand charges, utility service charges, and other recurring electricity operational expenses to the concerned electricity distribution utility/agencies to ensure uninterrupted operations of the ICCC ecosystem.

The Authority shall reimburse actual recurring electricity consumption charges on a monthly basis subject to:

- submission of original bills/invoices/receipts,
- submission of proof of payment,
- certification by the Authority's Authorized Representative,
- verification of actual deployment and operational status,
- and compliance with Contract and SLA obligations.

No reimbursement shall be admissible for penalties, delayed payment charges, interest liabilities, avoidable disconnection charges, unauthorized consumption, or inefficiencies attributable to the SI.

The SI shall ensure uninterrupted utility availability throughout the Contract Period and no operational disruption due to non-payment of utility charges shall be permissible.

13.5 Retention and Holdback

The Authority shall retain:

- Retention money;
- SLA-linked deductions;
- Penalties;
- Event-linked holdback amounts.

13.5.1 Minimum Retention

Minimum 15% of eligible payments shall be retained and linked with SLA compliance, Event Readiness Certification, and successful completion of Major Snan Day operations.

13.5.2 Event Protection Retention

Authority may withhold event-linked milestone payments in case of unresolved critical deficiencies, operational instability, cybersecurity non-compliance, or repeated SLA breaches during peak operational periods

14. PERFORMANCE SECURITY

The SI shall furnish an irrevocable Performance Bank Guarantee valid throughout implementation, warranty, O&M and extended support periods.

The Authority may invoke the PBG in case of:

- Material breach;
- SLA failure;

- Abandonment;
- Non-performance;
- Cybersecurity negligence;
- Failure during critical event operations.

15. INTELLECTUAL PROPERTY RIGHTS

All Project-specific deliverables including:

- Dashboards;
- Reports;
- Configurations;
- Metadata;
- GIS layers;
- Digital Twin models;
- AI datasets;
- Incident databases;
- Custom developments;
- SOPs;
- Network diagrams;
- Operational workflows;
  shall vest with the Authority.

The Authority shall have perpetual, irrevocable and royalty-free usage rights.

16. INFORMATION SECURITY AND CYBERSECURITY

The SI shall establish comprehensive cybersecurity controls including:

- Security hardening;
- MFA;
- RBAC;
- Encryption;
- SIEM integration;
- SOC integration;
- Endpoint security;
- Patch management;
- VAPT;
- Log monitoring;
- Incident response mechanisms;

- Ransomware protection;
- Backup protection;
- Network segmentation.

The SI shall comply with:

- CERT-In guidelines;
- MeitY guidelines;
- NCIIPC advisories;
- Applicable Government cybersecurity requirements.

16.1 Incident Response Timelines

Activity	Timeline
Detection	15 Minutes
Reporting	30 Minutes
Containment	1 Hour
Recovery	4 Hours

16.2 Security Audit

The Authority may conduct:

- Cybersecurity audits;
- Penetration testing;
- Forensic audits;
- Configuration audits;
- Source configuration verification.

17. CONFIDENTIALITY AND DATA PROTECTION

The SI shall:

- Maintain confidentiality of all operational data;
- Prevent unauthorized disclosure;
- Protect credentials and privileged access;
- Ensure data localization where mandated;
- Prevent unauthorized external hosting;
- Prevent data monetization or unauthorized analytics usage.

Confidentiality obligations shall survive termination.

18. AUDIT, ACCESS AND INSPECTION

The Authority or its authorized agencies may:

- Inspect sites;
- Inspect inventories;
- Audit systems;
- Review cybersecurity posture;
- Conduct surprise inspections;
- Verify manpower deployment;
- Conduct operational readiness reviews.

The SI shall provide unrestricted access during emergencies.

19. WARRANTY AND MAINTENANCE

19.1 Permanent Infrastructure

Comprehensive warranty and O&M shall be provided for 60 months.

19.2 Rental Infrastructure

Comprehensive support shall be provided during the deployment period.

19.3 Preventive Maintenance

The SI shall:

- Conduct scheduled preventive maintenance;
- Maintain spare inventory;
- Maintain critical spare availability during peak periods;
- Ensure MTTR compliance.

20. INSURANCE

The SI shall maintain:

- Third-party liability insurance;
- Transit insurance;
- Equipment insurance;
- Workmen compensation insurance;
- Cyber-risk insurance;
- Professional liability insurance.

Insurance policies shall remain valid throughout the Contract Period.

21. INDEMNITY AND LIMITATION OF LIABILITY

The SI shall indemnify the Authority against:

- Crowd disaster arising from system failure;
- Cybersecurity breaches;

- AI malfunction;
- Drone incidents;
- Operational negligence;
- Third-party claims;
- IPR infringement claims.

Limitation of liability shall not apply in case of:

- Fraud;
- Wilful misconduct;
- Cybersecurity negligence;
- Confidentiality breach;
- Data breach;
- IPR violations.

22. FORCE MAJEURE

Force Majeure shall include:

- Natural disasters;
- War;
- Civil disturbances;
- Epidemic;
- Government restrictions.

Cyber incidents shall not automatically qualify as Force Majeure unless proven beyond reasonable control of the SI.

23. EVENTS OF DEFAULT

Events of default shall include:

- Failure to achieve milestones;
- Repeated SLA failures;
- Project abandonment;
- Cybersecurity breaches;
- Fraud;
- Insolvency;
- Failure during major snan operations;
- Data tampering;
- Fake analytics generation;
- Non-availability of critical manpower;

- Failure in DR/failover testing.

24. TERMINATION

24.1 Termination for Default

The Authority may terminate the Contract in case of:

- Material breach;
- Persistent non-performance;
- Failure to achieve readiness;
- Cybersecurity negligence;
- Repeated critical outages.

24.2 Emergency Takeover Rights

During emergencies or public safety situations, the Authority may:

- Take temporary operational control;
- Access systems directly;
- Engage third-party operators;
- Use licenses and configurations;
- Utilize all operational resources.

25. EXIT MANAGEMENT

The SI shall ensure seamless transition including handover of Configurations; Passwords; Network diagrams; Source documents; AI models; Digital Twin datasets; GIS layers; VM images; Logs; Licenses; SOPs; and Asset registers.

The SI shall ensure uninterrupted services during transition.

26. DISPUTE RESOLUTION

Any dispute shall be resolved as follows:

Step 1: Amicable resolution within 15 days
Step 2: Escalation to senior committee within 15 days
Step 3: Arbitration under Arbitration & Conciliation Act, 1996

The language shall be English.

26.1 Amicable Settlement

Disputes shall initially be resolved through committee-level discussions.

26.2 Arbitration

Disputes unresolved within 30 days shall be referred to arbitration under Arbitration and Conciliation Act, 1996.

Seat of Arbitration: Ujjain/Bhopal, Madhya Pradesh.

26.3 Jurisdiction

Courts at Ujjain, Madhya Pradesh shall have exclusive jurisdiction.

PART B – SPECIAL CONDITIONS OF CONTRACT (SCC)

27. LIQUIDATED DAMAGES

Liquidated Damages may be imposed for:

- Delay in implementation;
- Delay in Go-Live;
- ICCC outage;
- AI analytics outage;
- OFC outage;
- Camera downtime;
- Failure during major snan days;
- Failure in DR readiness.

Indicative structure:

Failure	**LD**
Delay in Go-Live	Per Day Basis
ICCC Outage	Per Hour Basis
AI Analytics Failure	Escalating LD
OFC Failure	Escalating LD
Major Snan Failure	Severe LD

Maximum cumulative LD may extend up to 10% of Contract Value.

28. CHANGE CONTROL NOTE (CCN)

The Authority may:

- Increase or decrease quantities;
- Revise locations;
- Add integrations;
- Modify deployment strategy;
- Introduce additional event requirements.

All changes shall be documented through approved Change Control Notes.

29. RISK MANAGEMENT AND BUSINESS CONTINUITY

The SI shall establish comprehensive risk and continuity mechanisms including:

- Alternate ICCC;
- DR site;
- Redundant communication links;
- Alternate routing;

- Backup internet connectivity;
- Backup power systems;
- Emergency operation protocols;
- DR drills;
- Cyber recovery procedures.

The SI shall periodically conduct:

- Failover testing;
- Recovery drills;
- Operational continuity validation.

30. OEM RESPONSIBILITY

The SI shall ensure:

- Valid OEM support contracts;
- No end-of-support products;
- OEM-backed warranty;
- OEM onsite support during critical periods;
- L2/L3 escalation support;
- Lifecycle support availability.

31. MANPOWER AND DEPLOYMENT CONTROL

The Authority may require replacement of:

- Non-performing personnel;
- Personnel involved in misconduct;
- Personnel lacking required competency.

The SI shall ensure:

- Shift rosters;
- Biometric attendance;
- Minimum staffing levels;
- Emergency reserve manpower;
- Police verification.

PART C – SERVICE LEVEL AGREEMENT (SLA)

32. SERVICE LEVEL FRAMEWORK

SLAs shall apply to:

- ICCC operations;
- VMS platform;
- AI analytics;
- Digital Twin platform;
- Communication network;
- Cybersecurity systems;
- DR operations;
- Helpdesk services;
- Field infrastructure;
- Viewing centres;
- Crowd alert systems.

33. AVAILABILITY SLA

Component	Minimum Availability
ICCC Core Platform	99.5%
VMS Platform	99.5%
AI Analytics Platform	99.5%
Digital Twin Platform	99.5%
OFC Backbone	99.0%
Major Surveillance Cameras	98.0%

Major Snan Days may require enhanced SLA obligations up to 99.9%.

34. INCIDENT CLASSIFICATION

Severity	Description
Critical	Complete outage or public safety impact
Major	Significant degradation
Minor	Localized impact
Low	Non-critical issue

35. RESPONSE AND RESOLUTION SLA

Severity	Response Time	Resolution Time
Critical	5 Minutes	1 Hours

Major	15 Minutes	2 Hours
Minor	2 Hours	12 Hours
Low	1 Business Day	3 Business Days

36. PEAK SNAN DAY SLA

During Major Snan Days, the SI shall ensure:

- 99.9% uptime;
- Zero planned downtime;
- Dedicated war-room operations;
- Enhanced manpower deployment;
- Standby equipment;
- Rapid escalation;
- Mobile field response teams;
- Emergency communication channels;
- Continuous OEM support.

Any critical failure during peak operations shall attract severe penalties and may constitute Event of Default.

37. SLA PENALTY MATRIX

Non-Compliance	**Penalty**
ICCC Downtime	Hourly Deduction
Camera Downtime	Per Camera Per Day
OFC Outage	Escalating Penalty
AI Analytics Failure	High Penalty
Cybersecurity Non-Compliance	Critical Penalty
Major Snan Failure	Severe Penalty

Repeated SLA failure may lead to Enhanced penalties; Invocation of PBG; Blacklisting recommendation; Termination.

38. HELPDESK AND ESCALATION MANAGEMENT

The SI shall establish Centralized helpdesk; 24×7 support centre; Multilingual support; Ticketing system; Escalation matrix; Incident tracking system; Shift-wise operations.

The helpdesk shall support Incident logging; Escalation tracking; SLA monitoring; Reporting; Emergency escalation.

PART D – SCHEDULES AND ANNEXURES

Schedule / Annexure	Description
Schedule A	Scope of Work
Schedule B	Implementation Schedule
Schedule C	Payment Schedule
Schedule D	SLA Matrix
Schedule E	Manpower Deployment
Schedule F	Asset Register
Schedule G	Change Control Note
Schedule H	Cybersecurity Framework
Schedule I	DR and BCP Plan
Schedule J	Major Snan Operational Plan
Schedule K	Asset Handover
Schedule L	Escalation Matrix
Schedule M	Event Readiness Checklist
Annexure 1	Form of Agreement
Annexure 2	Non-Disclosure Agreement
Annexure 3	Integrity Pact
Annexure 4	Governance Framework
Annexure 5	Exit Management Plan