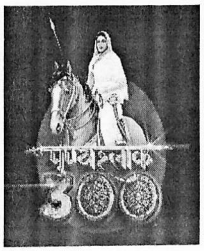
RIGHT TO INFORMATION

MAHATRANSCO
Maharashtra State Electricity Transmission Co. Ltd.

MAHARASHTRA STATE ELECTRICITY TRANSMISSION CO.LTD.
CIN NO. U40109MH2005SGC153646
Maharashtra State Load Dispatch Center

Tele :91-022-27601762 (P)
91-022-27601931 (O) Extn.1003
Email : cesldc@mahasldc.in
website : www.mahasldc.in

Office of The Chief Engineer
Maharashtra State Load Dispatch Center
Thane-Belapur Road, P.O. Airoli
Navi Mumbai Pin – 400 708.



Ref. CE/MSLDC/OP/DWS/ No 02197 **Date:** 14 OCT 2025

NOTIFICATION

Maharashtra State Load Despatch Centre (MSLDC), one of the oldest Load Despatch Centres in the country established in 1970, is the apex body for Grid Management in the State as per the provisions of the Indian Electricity Act-2003. In accordance with Section 32 of the Act, MSLDC is responsible for real-time operations for grid control and dispatch of electricity within the State to ensure secure and economic operation of the State grid.

To fulfill this mandate, it is essential to maintain real-time operational data along with daily and monthly reports through a robust Data Warehousing system. With the continuous rise in demand, supply, and infrastructure in Maharashtra, MSLDC intends to develop a comprehensive **cloud-based platform** covering:

1. Report Generation Software
2. Web-based Outage Management System
3. Web-based First-Time Charging (FTC)/Energizing Element
4. E-Logbook
5. Tripping Monitoring Portal

A document containing the primary functional and non-functional requirements is attached for reference.

Interested software developers with relevant expertise are invited to review the attached requirements and submit a Concept Document detailing implementation aspect of the proposed solution **by 28th October 2025.**

Any queries related to this notification must be submitted via email only to the below-mentioned address.

seop@mahasldc.in

Thanking You.

Yours faithfully,

(Girish Pantoji)
Chief Engineer (I/C)
MSLDC, Airoli.

Encl: As above.

Copy s.w.r.s. to:

- The Director (Operations), MSETCL, Mumbai.
- The Executive Director, MSLDC, Airoli, Navi Mumbai.

Development of comprehensive cloud-based platform for DSR (Daily System Report), Outage Management, FTC (First Time Charging), etc.

Introduction:

As per the clause 40 of MERC, State grid code Regulations, 2020, a daily/weekly/monthly report covering the performance of InSTS shall be prepared by SLDC based on the inputs from the Users and shall be put on MAHASLDC website. These reports contain the various information about Demand & supply scenario, Frequency profile, voltage profile, Generation/Transmission outages/trippings etc.

As per the clause 42.1.3 of MERC, State grid code Regulations, 2020, the objective of outage planning is *to optimize the transmission outages of the elements of State grid without adversely affecting the grid operation but considering the Generation outage schedule, outages of user/STU systems and maintaining system security standards*.

In view of above,

Maharashtra State Load Despatch Centre (MSLDC) shall establish a **Web-Based Data Warehousing System** consisting of reporting software module to centralize grid-generated data, enabling automated generation of periodic reports (Daily, Weekly, Monthly, Annual) for operations, planning, and regulatory compliance.

Maharashtra State Load Despatch Centre (MSLDC) shall implement a **Web-Based Outage Management System (WBOMS)** module to fully automate the outage planning process in compliance with Maharashtra's Standard Operating Procedure (SOP). The digital platform shall enable stakeholders to submit, track, and receive acknowledgments on outage proposals in real time.

In addition to above, **Maharashtra State Load Despatch Centre (MSLDC)** shall implement a **Web-Based FTC Module** for First-Time Charging & Integration of the elements in the Maharashtra grid. This module will facilitate the complete workflow for First-Time Charging (FTC) and integration of new or modified power system elements, aligned with POSOCO/NLDC and CERC regulations such as IEGC.

MSLDC shall implement a **Web-based Electronic Logbook (E-Logbook)** system to digitize and manage real-time control room operations, including shift handovers, event tracking, instructions management, and audit compliance.

MSLDC shall implement **Tripping Monitoring Portal** a centralized digital platform used by grid operators and utilities to track, analyze, and report/upload electrical grid disturbances, faults, and protection system activations (tripping). These portals are integral to ensuring grid reliability, compliance with regulatory standards, and facilitating timely corrective actions.

In view of this MSLDC is seeking for development of **comprehensive cloud-based platform for DSR (Daily System Report), Outage Management, FTC (First Time Charging), etc.**

The detailed scope of work is as mentioned below:

1. Web-Based Data Warehousing System:

MSLDC shall develop a web-based centralized software system to collect, compile, and manage operational data from all generation, transmission, distribution licensees, and Area/Sub-LDCs across Maharashtra. This system enabling MSLDC to generate periodic reports, analytics for grid planning, compliance, and strategic decision-making. A data warehousing system should offer flexibility in generating reports derived from its data.

Providing access to various of Data ware housing system to following entities/Users:

1. **Generation Licensees**: All Intra-State Generating Stations, Captive Generators, RE clusters
2. **Transmission Licensees**: MSETCL, Tata Power Transmission, Adani, JPTL, VIPL, etc.
3. **Distribution Licensees**: MSEDCL, Tata Power (D), AEML (D), BEST, Central Railways, and other deemed licensees
4. **Area/Sub-Load Despatch Centres (ALDCs/S-LDCs)** across Maharashtra as regional points of data submission
5. **There should be facility for ample numbers of users (say 5000 to 10000 users or so).**

Data fetching/ sharing /Integration with Following software:

1. MSLDC scheduling software – Bilateral power transaction data fetching through API
2. Fetching generating unit outages & Transmission element outages from Web based outage management module.
3. Incorporation of Business Intelligence (BI) and data analytics tool in software
4. Migration of data from existing modules of Data Warehousing Software i.e. DSR (Daily System Report), Outage Management, FTC (First Time Charging), E Logbook etc

Reports for external & internal Display:

State Daily System Report: -

1. State Daily System Report (DSR) Combined
2. Website Report
3. State Daily System Report (DSR) Individual reports
4. System Performance Report
5. Weekly system Report
6. Monthly Generation Report
7. Weekly and Monthly Declaration of Peak – off peak hours report
8. Monthly Bilateral Purchases
9. Periodical voltage profile
10. Unit wise monthly outages for generating stations
11. Monthly voltage profile for various generating stations
12. Monthly line outages
13. Day wise State Generation report with energy catered by Discoms
14. Day wise Maximum & Minimum Demand report of all Discoms
15. Month wise State Generation report with energy catered by Discoms
16. Month wise Maximum & Minimum Demand report of all Discoms
17. Export of Data for all the reports in State daily system report for required period
18. Various graphs, trend analysis.
19. Quary based dynamic reports and ad-hoc reporting.

20. Development of interactive dashboards, visualization using BI and Analytics Tool as per MSLDC requirement.

Mumbai Daily System Report: -

1. Mumbai Daily System Report (DSR) Combined
2. Mumbai Daily System Report (DSR) Individual reports
3. System Performance Report
4. Monthly Generation Report
5. Monthly Bilateral Purchases
6. Unit wise monthly outages for generating stations
7. Monthly line outages
8. Day wise Mumbai Generation report with energy catered by Discoms
9. Day wise Maximum & Minimum Demand report of all Discoms
10. Month wise Mumbai Generation report with energy catered by Discoms
11. Month wise Maximum & Minimum Demand report of all Discoms
12. Export of Data for all the reports in Mumbai daily system report for required period
13. Quary based dynamic reports and ad-hoc reporting.
14. Various graphs, trend analysis.
15. Development of interactive dashboards, visualization using BI and Analytics Tool as per MSLDC requirement.
16. Audit Trails: Logs of user activities for transparency and accountability.

2. Web-Based Outage Management System for Transmission elements & Generating units as per Standard outage procedure: -

The Maharashtra State Load Despatch Centre (MSLDC) is in the process of developing a web-based Outage Management System (WBOMS) to streamline and automate outage planning in accordance with Maharashtra's State Grid Code and Standard Operating Procedures (SOPs). This digital platform aims to enable generating companies and transmission entities to submit outage proposals, monitor approval statuses, and receive automated acknowledgments in real time, thereby enhancing coordination and reporting across stakeholders.

Web-Based Outage Management System should accept Planned & real time outage proposals from generating & transmission entities, provides transparent work flows and to facilitate interactions via web/mobile interfaces, and ensure compliance with regulator-mandated SOP.

Providing access of Data ware housing system to following entities/Users:

1. **Generation Licensees**: Intra-State Generating Stations
2. **Transmission Licensees**: MSETCL, Tata Power Transmission, Adani, JPTL, VIPL, etc.
3. **Main/Area/Sub-Load Despatch Centres (ALDCs/Sub LDCs)** across Maharashtra

Scope of work:

1. Processing & report generation of Day ahead outage proposals with SMS & auto email facilities
2. Processing & report generation of Emergency outage proposals with SMS & auto email facilities
3. Processing & report generation of Real time outage proposals
4. Processing & report generation of Flash Report

5. Processing & report generation of Occurrence Report
6. Processing & report generation of Monthly Planned outages (Both OCC & MOCM)
7. Processing & report generation of Annual Outages
8. Processing & report generation of POST OCC outages
9. Abstract of availed/deferred/not availed outages for both OCC approved & State element outages
10. Report generation of element wise outage abstract
11. Outage availed data to be linked with State Daily system Report
12. Generation of Important – Non-important element list
13. Processing of Transmission system availability certification for all transmission licensees
14. Report generation for project related outages
15. Quary based dynamic reports and ad-hoc reporting.
16. Various graphs, trend analysis.
17. Development of interactive dashboards, visualization using BI and Analytics Tool as per MSLDC requirement.
18. Audit Trails: Logs of user activities for transparency and accountability.

3. Web-Based First Time Charging as per procedure: -

A Web-Based First Time Charging (FTC) module should be online application designed for registered transmission licensees and generating companies to digitally manage every step of the trial-run/energization submission as per CERC-mandated procedure. This includes intake of applications, annexure upload, multi-tier scrutiny, real-time acknowledgments, digital consents, and post-energization audit trails.

Providing access of Data ware housing system to following entities/Users:

1. **Generation Licensees**: Intra-State Generating Stations
2. **Transmission Licensees**: MSETCL, Tata Power Transmission, Adani, JPTL, VIPL, etc.
3. **Main/Area/Sub-Load Despatch Centres (ALDCs/Sub LDCs)** across Maharashtra

Scope of work:

- **User Registration Module:**
  • Secure sign-up and authentication (email/SMS OTP).
  • Profile management and password recovery.

- **Input & Document Upload Interface:**
  • Incorporation of element details
  • File upload support for relevant documents (PDF, JPG, DOC, etc.).
  • Automated SMS and email confirmations upon submission.

- **Automated Annexure Generation**:
  • System-generated annexures based on data inputs (Annexure A, B, C, etc.).

- **Departmental Workflow Processing**:
  • Routing of submission packets to respective departments.

• Status updates, review/approve/reject actions tracked per department.
• Consent capture from all departments.

- **Final Format IV Generation**:
  • Upon inter-departmental approval, auto-generate Format IV document.

- **Flash Report After Energization**:
  • Post-energization, generate flash report summarizing essential outcome metrics.

- **Audit Trails: Logs of user activities for transparency and accountability.**

4. E-logbook: -

An E-logbook should be online application which is digital equivalent of a traditional paper log, providing an organized, secure, and easily managed record-keeping system.
Key capabilities:

- Real-time data entry, storage, and retrieval
- Access via cloud or offline devices
- Automatic validation, audit trails, and timestamping

Providing access of E-logbook to following entities/Users:

1. **Main/Area/Sub-Load Despatch Centres (ALDCs/Sub LDCs)** across Maharashtra

Scope of work:

- **Notice Board for System Highlights**
- Notice board module to display timely headlines, notable trends or alerts.
- Admin interface: add/edit/remove notices in real time, set display timelines (e.g. till date).

- **Koyna Generation Information**
- Real-time & historic generation data

- **Incorporation of Load-Shedding Details**
- **Load-shedding schedule entries**: date/time, affected regions/areas, duration, load impact (MW).
- **Analytics**: quantify total load shedding hours, affected load, frequency, and trend over the period.

- **Abstract of All Reports for the Required Period**
  - Quary based dynamic reports and ad-hoc reporting.

- **Audit Trails: Logs of user activities for transparency and accountability.**

5. Tripping Monitoring Portal: -

A Tripping Monitoring Portal should be centralized digital platform to be used by grid operators and utilities to track, analyze, and report/upload electrical grid disturbances, faults, and protection system activations (tripping). This portal should be integral to ensuring grid reliability, compliance with regulatory standards, and facilitating timely corrective actions.

Providing access of Data ware housing system to following entities/Users:

1. **Generation Licensees**: Intra-State Generating Stations
2. **Transmission Licensees**: InSTS like MSETCL, TPCL-T, MEGPTCL, JPTL, VIPL, etc.
3. **Main/Area/Sub-Load Despatch Centres (ALDCs/Sub LDCs)** across Maharashtra

Scope of work:

- **User Authentication**: Secure login mechanisms for authorized personnel.
- **Event Dashboard**: Visual representation of ongoing and past grid events.
- **Data Upload Interface**: Facilities for utilities to submit FIR, DR, and EL outputs.
- **Reporting Tools**: Generation of Flash and Detailed Reports post-grid events.
- **Alert System**: Notifications for pending submissions or compliance deadlines.
- **Audit Trails**: Logs of user activities for transparency and accountability.

While developing a Data ware housing system, consider the following:

- **Regulatory Compliance**: Ensure alignment with national, state grid codes and CEA standards.
- **Data Security**: Implement robust cybersecurity measures to protect sensitive information.
- **User Training**: Provide comprehensive training for all stakeholders on portal usage and protocols.
- **Integration Capabilities**: Ensure compatibility with existing grid management and protection systems.
- **Scalability**: Design the portal to accommodate future expansions and technological advancements.

6. Bidder is supposed to hand over the complete, fully tested/ audited, bug free, final version of source code (in softcopy format), module wise user manuals hard copy as well as soft copy integrated as help menus within the Data Warehousing System Web Application. Software documentation should have unique management defined documentation numbering intellectual.
The Bidder shall host the Data Warehousing System Web Application Software on cloud. The Bidder shall also arrange the Pre-Production environment (development and testing environment) along with required licenses for development, testing and further modification or revision of Data Warehousing System Web Application software. MSLDC shall not arrange any hardware for this requirement.

The functional requirement, system architecture and integration with other existing software and hardware requirement for cloud hosting for the proposed system is detailed in this Document. The bidders are requested to understand the functional requirement in detail and if required, they may visit MSLDC for any clarification / understanding of existing system as well as proposed Data Warehousing System Web Application.

The Proposed MSLDC Data Warehousing System Web Application shall needs to be developed using a robust open source software platform. The operating system (OS),

programming language, database systems, etc required to develop the web application software shall be choice of the bidder. However, shown below table highlights the preferred open source technologies platform for development of the Data Warehousing System Web Application.

Preferred Technology Platforms

S.No	Development Platform	Open Source Solution or Licensed Enterprise Solution
1.	Application Server Software	Open Source Technologies (Preferably JAVA based)
2	Application Server Operating System	Linux Enterprise edition
3	Database Server Software	High performance Database Software Oracle Standard or Enterprise Edition/ Postgre Enterprise/ MySql Enterprise (Latest Version)
4	Database Server Operating System	Linux Enterprise edition
5	Database Connectivity Methods	Native Connectivity

7. ACCEPTANCE TEST PLAN & PROCEDURE FOR UAT

7.1 User Acceptance Tests (UAT) Activities:

User Acceptance Test:

1. User Acceptance Tests (UAT) of the DWS Software Application along with its integration with existing systems at MSLDC shall be completed by the Bidder as specified in the TO-BE architecture specified in the design documentation.

2. The User Acceptance Tests (and repeats of such tests) shall be the responsibility of the Bidder, and shall be conducted in coordination with MSLDC during Commissioning of DWS Software Application along with its integration with existing systems at MSLDC. The UAT shall meet but not restricted to the Technical Requirements and the MSLDC's performance requirements.

3. The UAT shall be conducted in accordance with the test scripts approved by the MSLDC.

4. The Bidder may give a notice to the MSLDC requesting the issue of a User Acceptance Certificate after conducting the UAT as per the requirement of these Technical Specifications.

5. After receipt of the Bidder's notice, the MSLDC shall within a reasonable period of time issue a User Acceptance Certificate; or Notify the Bidder in writing of any defect for deficiencies or other reason for the failure of the UAT.

6. The Bidder shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies and/or other reasons for the failure of the UAT. Once the Bidder has made such remedies, it shall notify the MSLDC, and the MSLDC, with the full cooperation of the Bidder, shall carry out re-testing (UAT) of the DWS Software Application along with its integration with existing systems at MSLDC.

7. Upon the successful conclusion of the UAT Tests including successfully complying all integration touch points, the Bidder shall notify the MSLDC of its request for User Acceptance Certification for complete DWS Software Application along with its integration with existing systems at MSLDC. MSLDC shall issue the User Acceptance Certification (signed by respective owner), in accordance with RFP or notify the Bidder of further defects, deficiencies, or other reasons for the failure of the User Acceptance Test. The procedure set out in this RFP shall be repeated, as necessary, until a User Acceptance Certificate is issued.

8. Production use (Go Live) shall not commence prior to the formal User Acceptance Testing.

7.2 Pilot Run / Stabilization:

1. Stabilization Period will start after the UAT of the concerned application over i.e. the DWS Software Application along with its integration with existing systems at MSLDC and cloud solution is over.

2. The Stabilization Acceptance Tests (SAT) (Performance Guarantee Tests and repeats of such tests) shall be the responsibility of the Bidder, and shall be conducted in coordination with MSLDC after stabilization period of the DWS Software Application along with its integration with existing systems at MSLDC, to ascertain whether the DWS Software Application along with its integration with existing systems at MSLDC meets the MSLDC's performance requirements and complete functionality as desired by MSLDC. Stabilization shall also include the stabilization of DWS Software on cloud.

3. Stabilization Acceptance will only be provided after cloud resources are provisioned and cloud hosting testing (as applicable) has been completed, which will include but not limited to
    1. Switch over of application from Data centre (DC) to Disaster Recovery (DR) as per defined RTO and RPO
    2. Switch over applications from DR to DC as predefined RTO and RPO
    3. Complete Data Replication and Reverse Data Replication as per RPO
    4. Fully functional application while DR site is operational as confirmed by MSLDC end users of application.

4. Stabilization Acceptance would also involve Testing of Cloud back to the DR site located at different Geographical location as provisioned by the CSP provider.

5. At MSLDC's discretion, Stabilization Acceptance Tests may also be performed on upgrades and new version, releases that are added or field-modified.

6. If the system is found to be lacking in meeting Performance guarantee parameters requirements, deduction on account of Liquidated Damages & Penalties as per the contract will be levied.

7.3 GO-LIVE Activities:

1. After the issue of the User Acceptance & Stabilization Certificates for all applications the Bidder will commence Go-Live Acceptance Test (after successful operation & stabilization for all applications) to ensure that the Cloud Service Solution is rolled out in totality and all integration requirements are compiled in accordance with the specified timelines.

2. The Go-Live Acceptance Tests shall be the primary responsibility of the Bidder, but shall be conducted in consultation with MSLDC. During Go Live of DWS Software Application, Bidder shall ensure the operation of DWS Software along with its integration with existing software at MSLDC and hosting of DWS Software on cloud, meets the technical requirement as specified in this Tender Document.

3. Tests shall be conducted in accordance with the test scripts approved by MSLDC. At MSLDC's discretion, Go-Live Acceptance Tests may also be performed on upgrades and new version, releases that are added or field-modified after User Acceptance of the "Cloud Service Solution".

4. Bidder shall be responsible for the security audit of the proposed DWS software application as per the guidelines specified by Indian Computer Emergency Response Team (CERT-In). The security audit agency shall be an empaneled agency in CERT-In. cyber security audit certificate shall be provided by the bidder before acceptance of the system as well as renewal of the same during complete Contract period.

7.4 Go-Live Acceptance:

1. Go-Live Acceptance shall occur in respect the DWS Software Application along with its integration with existing system at MSLDC and hosting of DWS Software on cloud, when all the UAT and SAT have been successfully completed.

2. The Bidder may give a notice to the MSLDC requesting the issue of the Go-Live Acceptance Certificate along with all the necessary documents to justify Bidder's claim of completion of UAT and SAT.

3. After receipt of the Bidder's notice, the MSLDC shall:
    a. Issue a Go-Live Acceptance Certificate; or
    b. Notify the Bidder in writing of any defect or deficiencies or other reason for the failure of the Go-Live Acceptance Tests.
4. If the system doesn't get stabilized within stipulated period, the Bidder shall rectify the defects within the reasonable time as accepted to MSLDC, at no extra cost and again host the DWS Software on the Cloud as per the provisions of Technical Specifications of this Tender document

7.5 Fall Back:

If the System or Subsystem fails to pass the UAT, Go-Live or Operational Acceptance Test(s) even after 3 unsuccessful attempts, then MSLDC reserved the right to terminate the Contract and if the Contract is terminated the Performance Bank Guarantee (PBG) will be forfeited. The remaining work shall be carried out by MSLDC through any other vendor at the risk and cost of the Bidder

7.6 Performance Guarantee Tests and Penalty Provisions:

The Dataware housing system (DWS) software application developed over its individual software modules is expected to perform the activities within the desired timeline given below in the Table for each module. If the Software does not perform as per the performance norms specified in the following Tables, the appropriate penalty shall be applicable. During the Contract Period the Performance shall be monitored as per the Tables below and the Penalty shall be calculated and shall be deducted from the balance amount of software development to be paid after competition of Warranty Period.

A. Timelines for Report generation Activities within Web-based Data ware housing Module:

Sr.No.	Report Generation Activity	Expected Time	Severity level	Applicable Penalty
1	Home Page / login page opening	1-2 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
2	After login with user account credentials, dashboard opening	4-5 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
3	Menu Navigation	1 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
4	Discom demand upload / update	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
5	Data aggregation (background calculation)	Immediate after data updating message pop up	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
6	Any report opening	5-7 sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
7	Transferring Bilateral power to DWS	Immediate (Automatic)	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
8	Processing of data for any report generation	5-7 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted

B. Timelines for Outage processing Activities within Web-based Outage Management System Module: -

Sr.No.	Outage Processing Activity	Expected Time	Severity level	Applicable Penalty
1	Home Page / login page opening	1-2 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
2	After login with user account credentials, dashboard opening	4-5 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
3	Menu Navigation	1 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
4	Creation / updation of outage proposal	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
5	Approval/Deferrement of outage proposal	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
6	Data transfer within two accounts (background activity)	Immediate after data updating message pop up	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
7	Submission of consolidated Day ahead outage proposals	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
8	Generation of SLDC Code	1 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
9	Any report opening	5-7 sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
10	Any document /image upload/update	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
11	Generation of auto mail & SMS	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted

C. Timelines for First Time Charging Activities within Web-Based First Time Charging (FTC) Module: -

Sr.No.	First Time Charging Activity	Expected Time	Severity level	Applicable Penalty
1	Home Page / login page opening	1-2 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
2	After login with user account credentials, dashboard opening	4-5 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
3	Menu Navigation	1 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
4	Document / images to upload	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
5	Processing of data	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
6	Generation & opening of Annexures & Formats	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
7	Transfer of element in Master data of DWS	1 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted

D. Timelines for real time activities in E-logbook Module: -

Sr.No.	Real time activity in E-logbook	Expected Time	Severity level	Applicable Penalty
1	Home Page / login page opening	1-2 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
2	After login with user account credentials,	4-5 Sec	Medium	If service level is not maintained for more than 3 times during the

	dashboard opening			month, the payment of 1% of Monthly AMC Charges shall be deducted
3	Menu Navigation	1 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
4	Generation of SLDC Code	1 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
5	Report generation & opening	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted

E. Timelines for tripping Activities within Tripping Monitoring Portal:

Sr.No.	Tripping Activity	Expected Time	Severity level	Applicable Penalty
1	Home Page / login page opening	1-2 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
2	After login with user account credentials, dashboard opening	4-5 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
3	Menu Navigation	1 Sec	Medium	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
4	Uploading of documents / files/images	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
5	Generation / opening of reports	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted
6	Generation of notification for pending submission	1-2 Sec	High	If service level is not maintained for more than 3 times during the month, the payment of 1% of Monthly AMC Charges shall be deducted

SCOPE OF WORK

The Scope of work for this RFP would be under the following broad categories but is not limited to

- Development of Data Warehousing System
- Cloud Hosting of Data Warehousing System
- System Administration of Data Warehousing System
- Annual Maintenance Services for Data Warehousing System
- Change Request
- OS, Database & other applications Management
- Cyber Security Audit of Data ware housing system web application
- Security and Statutory Requirements
- Documentation Requirement

Detailed description of the Scope of work is as under:

1. Development of Data Warehousing System

Sample Project Schedule

The bidder shall produce a detailed project plan and details of resource allocations in line with expectations of timelines defined below. This plan should provide overall schedule of requirements, timelines, dependencies, deliverables, and milestones.

<< Sample Schedule as below to be modified as per the requirement >>

Sr. No.	Milestone	Timeline (Tentative)	Deliverables
1	SRS Preparation & Sign off Prototype Preparation & Sign off	__ Weeks	01. SRS
2	Development and Testing (Monthly release of web Applicaton in Agile model)	__Weeks	01. Monthly Release Report
3	1. User Acceptance Testing (UAT) 2. Closure of the observations based on UAT feedback	__ Week	01. Test Cases Report, 02. UAT Observation Closure Report, 03. Cyber Security Audit, Observations report, 04. Cyber Security Audit Certificate, 05. Design Document (Cloud) 06. Final Source Code 07. Go-Live Report.
4	1. Cyber Security Audit 2. Closure of the observations identified in Security Audit		
5	Hosting in Cloud Server, SSL certificate, Domain name integration, etc.		
6	Go-Live of Applicaton		
7	Hypercare period (Postproduction Support)	_ Weeks	Hypercare Period Report
8	Warranty Period	_ Year	Preventive Maintenance Report.

Web Application Security of the Data Warehousing System

- Web Application developed should be GIGW 3.0 compliant.
- Bidder shall take necessary measures to ensure the Application Programming Interface (API) Security.
- Bidder shall take necessary measures to ensure the Cloud Services Security.

- Bidder shall follow the guidelines as per Annexure 'F' to improve cyber posture of the Web Application.

2. Cloud Hosting of Data Warehousing System

- The Bidder shall be responsible for selection and hosting of the proposed **Data ware housing system** web-based application on cloud through MeitY empaneled Cloud Service Provider (CSP). The Bidder shall be the single point of contact for the MSLDC for interaction with the CSP solution provider or the Network Bandwidth Service Provider (NBSP) offered by the Bidder.
- The Bidder will be responsible for providing required IT infrastructure for hosting Data ware housing system web-based application in at least Tier III data centre within India.
- You shall deploy the proposed **Data ware housing system** web application on the as DC+DR type with the following environments with minimum infrastructure as specified below in dedicated as well as isolated instances. Detailed server specification shall be as per the **Annexure 'A'**.
  - Production (1 App Server + 1 DB Server in HA)
  - UAT (1 Server App + DB)
  - Disaster Recovery (1 App Server, 1 DB Server)
- The above environments are to be deployed on the Cloud Environment with dedicated instances with reserved capacity for minimum Six years
- Data ware housing system web application shall be deployed on Enterprise Linux platform as per the specification in **Annexure 'A'**
- You shall also provide the services as per the **Annexure-'B'**
- Each of the environments mentioned above should be logically isolated, i.e., separate from the production environment in a different VLAN than the Pre-production/UAT environment
- CSP shall not provide any unmanaged VMs for the Data ware housing system web application.
- Cloud Solution should be flexible and dynamic in nature. It should provide APIs to interface with third-party modules / applications. It is expected that the Data Warehousing Web Application shall easily and readily interface with third party systems and modules applications.
- The Cloud Solution should provide horizontal, vertical and linear scalability without inherent bottle necks and core design changes.
- The Cloud Solution should have High real-time performance and throughput.
- The solution should have high availability for Data Warehousing Web Application along with other integrated applications.
- The selected Bidder shall be a single point of contact for any issues in Solution implemented, Hardware, Operating System, Database, Performance, Integration etc for entire contract period.
- The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines as and when published).
- The Bidder shall be responsible for providing the best suitable Cloud Infrastructure

(server/virtual machines), storage for hosting Data Warehousing Web application which shall needs to be integrated with software applications operational at MSLDC for the purpose of Data Warehousing Web Application implementation.

- The selected Bidder shall be a single point of contact for any issues in Solution implemented, Hardware, Operating System, Database, Performance, Integration etc for entire contract period i.e. during Warranty and AMC Period. You shall be responsible for management & maintenance of the complete solution provided.
- During contract period i.e. Warranty and AMC Period, You should provide sufficient capacity on Cloud platforms in terms of data processing, data storage and network bandwidth to handle the overall load and traffic coming to the Data warehousing System without compromising the overall performance of the system.
- It will be the responsibility of Solution Provider to prepare the specification for cloud platform i.e. CPUs, RAM, storage, required software, other equipment and the network requirements for running the Data warehousing System efficiently. Whatever infrastructure is needed shall be clearly accounted in the bid document
- The cloud service should provide dedicated IP, dedicated SSL/ TLS certificate.
- Before deployment of the Data warehousing system web-based application into the cloud, a detailed IT architecture shall be submitted by the CSP through Bidder. The design document must essentially (but not limited to) included:-
    - Cloud Instances/VMs, Storage, Additional Services Overview
    - Cloud System configurations for VMs and Storages
    - Cloud Architecture diagram for Data ware housing system
    - Physical details of each Cloud component
    - Overall Cloud networking scheme
- The Bidder should prepare and submit a detailed implementation plan with mapping of infrastructure at DC site and DR site including following parameters:
    - Server Provisioning
    - Storage Requirements
    - Network interfaces requirement
    - Network throughput requirement
    - Adequate Power and Backup requirement
    - Failover mechanism for replication links

    On acceptance of implementation plan by MSLDC the Bidder shall implement the cloud solution and offer for testing.
- The Bidder shall be responsible for implementation of Disaster Recovery (DR) as a Services (DRaaS) for the Data ware housing system software. The bidder shall be responsible for bringing up the DR service as per the Recovery Point Objective (RPO) and perform back up of data as per Recovery Time Objective (RTO) mentioned. RPO should be less than or equal to <<30 Minutes>> and RTO shall be less than or equal to <<2 hours>>.
- The Bidder shall offer DR as a service for all resources offered on primary DC site. The Bidder shall be responsible for provisioning of bandwidth for replication of data between the DC site and DR Site. The SLA for the replication of data will be attributed to the Bidder. The RPO during disaster recovery shall be <=30 Minutes and RTO shall be <=2 Hours.

- Geographical Location of the Disaster Recovery Environment shall be different location from the Data Center environment.
- In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. Website data and website states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO.
- Bidder shall formulate an effective Back-up Strategy and Disaster Recovery Plan and shall be responsible for implementing the same at the time of go-live of Data ware housing system.
- Bidder shall also ensure that the hosting services should be portable to another vendor without any changes to hosting environment.
- You shall provide the Provide business continuity services in case the primary site becomes unavailable.
- In the event of a disaster at DC site, activation of services from the DR site is the responsibility of Bidder. The Bidder shall develop appropriate policy, checklists in line with ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate DR site. DR drills needs to be performed by the Bidder at least twice a year (six monthly) to check disaster preparedness and need to submit the report to MSLDC.
- Bidder should have solutions to route Internet users seamlessly from Cloud Platform to DR site (if required).
- Bidder should have Certified Cloud Administrator, Linux certified Systems Administrator, Certified Database Administrator on the roll.
- MSLDC retains ownership of all virtual machines, templates, clones, and scripts/applications created for the Data ware housing system web application and its interconnections. MSLDC retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.
- MSLDC retains ownership of Data ware housing system web application and it's inter connected applications installed on virtual machines and any application or product that is deployed on the Cloud by the MSLDC.
- MSLDC shall retain ownership of any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.
- MSLDC shall be provided access rights (including the underlying secure connection) to the user administration / portal of cloud services to have visibility into the dashboard, SLAs, management reports, etc. provided by the Cloud Service provider.
- CSPs shall provide interoperability support with regards to available APIs, data portability etc. for the MSLDC to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or Disaster Recovery (DR) services from a different service provider.
- CSP should adhere to the ever evolving guidelines as specified by CERT-In (http://www.cert-in.org.in/)
- CSP should adhere to the relevant standards published (or to be published) by MeitY or any standards body setup / recognized by Government of India and notified to the CSP by MeitY as a mandatory standard.
- CSP should be MeitY empaneled throughout the contract period

- Compliance process to the defined international standards and security guidelines such as ISO 27001, for maintaining operations of cloud and ensuring privacy of MSLDC data should be followed by the bidder
- The bidder shall design and implement a change release management and configuration management procedure in consultation with MSLDC to process any change to the cloud environment services and its hosted applications. This procedure must include the capability to support the transition between the pre-production environments prior to release to the production environment.
- Provide physical and virtual access to the technical persons of MSLDC.
- The Bidder will be responsible for provisioning of requisite network infrastructure (including switches, routers and firewalls) to ensure accessibility of the servers as per defined SLA's.

- **IMPORTANT NOTE**
  - The proposed solution must be capable to incorporate Information Security, Business Continuity and Data Privacy controls as mandated by Regulations and Industry standards (including but not limited to ISO27001, ISO22301, GAPP etc.).
  - The bidder is responsible for arriving at the sizing of Hardware independently, based on volume provided by MSLDC. MSLDC is not responsible for any assumption made by the bidder. If the solution does not meet the performance/service level as desire in the RFP, the bidder will be responsible to carry out the necessary scale-up of Hardware on cloud, without any additional cost to MSLDC during the contract period.
  - The bidder is responsible for arranging the required infrastructure along with required licenses for development of the Data Warehousing Web Application without any additional cost to MSLDC. Cloud hosting charges shall be applicable from the date of successful go-Live of the Data Warehousing Web Application.
  - The bidder is responsible for arranging the required license along with its subscription for Data Warehousing Web Application, in all the environment of DC & DR without any additional cost to MSLDC during the contract period.
  - The Bidder must plan, assist, guide and formulate strategy for System Integration and User Acceptance Testing along with Audits (third party/ internal audits) of the proposed solution.

3. System Administration of Data Warehousing System

Successful Bidder has to provide Systems Administration for entire contract period (Warranty and AMC) by coordinating with CSP provider. Systems Administration task shall include but not limited to

- **Database Administration**: Successful Bidder has to provide DBA Support for entire contract period (Warranty and AMC).
  - ✓ Pro-active Monitoring System: To Achieve Maximum Uptime and Optimum database Performance as per the schedule to be provided by MSLDC.
  - ✓ Database Administrative Task: General DBA task for day-to-day smooth operation.
  - ✓ Patch Management: To be at par in industry and always be current on technology and Security.
  - ✓ Backup and Recovery: To ensure better recoverability from database losses as per

the schedule to be provided by MSLDC

- ✓ Space Management: To ensure space availability in the database for continued service and can avoid application outages.
- ✓ Database Log and Trace file Management: Database trace/log files housekeeping.
- ✓ Performance Management: To ensure better Database performance
- ✓ Online Service Request System: To ensure timely response to the request and keep record for future analysis. It is the responsibility of successful bidder to generate Service Request with OEM.
- ✓ Database Planning and Re-Designing: To ensure current industry standard for database infrastructure for the better Business functionality.
- ✓ Reports: Monthly Health Check-up report of DBA.
- ✓ Any other / DBA activities to run the system as per SLA specified in this document.

- **Business Continuity Services**
  - ✓ Provide business continuity services in case the primary site becomes unavailable.
  - ✓ The Bidder shall be responsible for implementation of Disaster Recovery (DR) as a Services (DRaaS) for the Data ware housing system software. The bidder shall be responsible for bringing up the DR service as per the Recovery Point Objective (RPO) and perform back up of data as per Recovery Time Objective (RTO) mentioned. RPO should be less than or equal to <<30 Minutes>> and RTO shall be less than or equal to <<2 hours>>.
  - ✓ The Bidder shall offer DR as a service for all resources offered on primary DC site. The Bidder shall be responsible for provisioning of bandwidth for replication of data between the DC site and DR Site. The SLA for the replication of data will be attributed to the Bidder. The RPO during disaster recovery shall be <=30 Minutes and RTO shall be <=2 Hours.
  - ✓ Geographical Location of the Disaster Recovery Environment shall be different location from the Data Center environment.
  - ✓ In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. Website data and website states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO.
  - ✓ Bidder shall formulate an effective Back-up Strategy and Disaster Recovery Plan and shall be responsible for implementing the same at the time of go-live of Data ware housing system.
  - ✓ In the event of a disaster at DC site, activation of services from the DR site is the responsibility of Bidder. The Bidder shall develop appropriate policy, checklists in line with ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate DR site. DR drills needs to be performed by the Bidder at least twice a year (six monthly) to check disaster preparedness and need to submit the report to MSLDC.
  - ✓ Bidder should have solutions to route Internet users seamlessly from Cloud Platform to DR site (if required).

- **Security Administration-**
  - ✓ Appropriately configure the security groups in accordance with the standard

networking policies.

- ✓ Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.
- ✓ Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.
- ✓ Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorised activity.
- ✓ Perform regular security monitoring to identify any possible intrusions
- ✓ Bidder to notify the MSLDC promptly in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data
- ✓ The Bidder shall report forthwith in writing of information security breaches to the MSLDC by unauthorized persons other than authorised by MSLDC (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential Information
- ✓ The Bidder undertakes to treat information passed on to them under this Agreement as classified. Such Information will not be communicated / published / advertised by the Bidder to any person/organization without the express permission of the MSLDC.
- ✓ The Bidder shall be responsible for ensuring security of Data ware housing system web application and infrastructure from any threats and vulnerabilities.
- ✓ The Bidder shall address ongoing needs of security management including, but not limited to, monitoring of various devices / tools and vulnerability protection through implementation of proper patches and rule
- ✓ Bidder shall be responsible for managing specific controls relating to shared touch points within the security authorization boundary, such as establishing customized security control solutions. Examples include, but are not limited to, configuration and patch management, vulnerability scanning, disaster recovery, and protecting data in transit and at rest, host firewall management, managing credentials, identity and access management, and managing network configurations.

- **Monitoring Performance and Service Levels**
  - ✓ The Bidder shall provision monitoring tools for measuring the service levels, application performance and utilization, server performance and utilization, storage performance and utilization and network performance and utilization. The tool shall be capable of providing the exact utilization of servers and shall be able to generate per day, per month and per quarter utilization reports.
  - ✓ Provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.
  - ✓ Reviewing the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels.
  - ✓ Monitoring of service levels, including availability, uptime, performance, application specific parameters, e.g. for triggering elasticity, request rates, number of users connected to a service.
  - ✓ Detecting and reporting service level agreement infringements.
  - ✓ Monitoring of performance, resource utilisation and other events such as failure of

service, degraded service, availability of the network, storage, database systems and operating Systems including API access within the cloud service provider's boundary.

- ✓ Overall monitoring of the deployed network bandwidth/ links so as to ensure the desired uptime. In case of downtime/ link failure, reporting immediately the same to the Network Bandwidth Provider (NBP) and tracking until the link is restored and services are operational as required.
- ✓ Perform daily system monitoring, verifying the integrity and availability of cloud resources, Cloud Services and key processes, reviewing system and application logs, and verifying completion of scheduled jobs such as backups.
- ✓ Monitoring the uptime, performance, resource utilization of the cloud resources assigned for Data ware housing system web application.
- ✓ Enable the logs and monitoring as required to support for third party audits.

- **Backup**
  - ✓ You shall Configure, schedule, monitor and manage backups of all the data including application and database but not limited to files, images and database.
  - ✓ Perform daily backup operations, ensuring all required file systems and system data are successfully backed up to the appropriate media, recovery tapes
  - ✓ Restore from the backup where required.
- **User Administration**
  - ✓ Management of user in the OS level and firewall level will be take care by CSPs/bidder.
  - ✓ Properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks.
  - ✓ Create, change, and delete user accounts per request

- **Support for third party audits**
  - ✓ Enable the logs and monitoring as required to support for third party audits

- **MIS Reports**

  Bidder shall submit the reports on a regular basis in a mutually decided format. The Bidder shall workout the formats for the MIS reports and get these approved by the MSLDC after awarded the contract. The following is only an indicative list of MIS reports that may be submitted to the MSLDC. Monthly Reports
  - ✓ Component wise server as well as Virtual machines availability and resource utilization
  - ✓ Consolidated SLA / Non- conformance report.
  - ✓ Summary of component wise uptime.
  - ✓ Log of preventive / scheduled maintenance undertaken
  - ✓ Log of break-fix maintenance undertaken
  - ✓ All relevant reports required for calculation of SLAs

- **Usage Reporting-**
  - ✓ Track system usage and usage reports
  - ✓ Monitoring, managing and administering the terms of SLAs.
  - ✓ Provide the relevant reports including real time as well as past data/information/reports to validate the SLA related penalties.
  - ✓ Provide the Access Log report.

- **Resource Management**
  - ✓ Adequately size the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels.
  - ✓ While the initial sizing & provisioning of the underlying infrastructure may be carried out based on the information, provided in the Indicative Bill of Material Clause 6.6. Subsequently, it is expected that the CSP/bidder, based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute, memory, and storage as per the performance requirements of the solution.
  - ✓ For any major expected increase in the workloads, carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution.
  - ✓ Bidder is required to ensure provision of additional VM's, Memory, Storage etc when the utilization exceeds 80%
  - ✓ Bidder shall Manage the instances of storage, compute instances, and network environments. Bidder is also responsible for managing specific controls. Examples include, but are not limited to, configuration and patch management, vulnerability scanning, disaster recovery, and protecting data in transit and at rest, host firewall management, managing credentials, identity and access management, and managing network configurations.

- **Patch & Configuration Management**
  - ✓ Manage the instances of storage, compute instances, and network environments. Service Provider is also responsible for managing specific controls relating to shared touch points within the security authorization boundary, such as establishing customized security control solutions. Examples include, but are not limited to, configuration and patch management, vulnerability scanning, disaster recovery, and protecting data in transit and at rest, host firewall management, managing credentials, identity and access management, and managing network configurations.
- **Miscellaneous-**
  - ✓ Installation/Upgradation of resources, operating system (OS), softwares and selection of appropriate services based on compute, data, or security requirements. Upgrade and re-configure cloud system as per the operational needs.
  - ✓ Planning and approval for additional cloud resources by consulting with MSLDC for change requests associated with modification in Data ware housing system web application.
  - ✓ Document cloud configuration and installation procedures. Bidder will be

responsible for the availability, security, access, backup, and performance of the cloud infrastructure.

- ✓ View and analyze summary data on cloud resource deployments. Monitor requests and key metrics for cloud resources
- ✓ Plan, coordinate, and implement network security measures in order to protect data, software and network configurations.
- ✓ Perform ongoing VM performance tuning, software upgrades, and resource optimization as required. Configure CPU, memory, and disk partitions as required. Perform periodic performance reporting to support capacity planning.
- ✓ Detailed Systems Administration activities shall be provided to successful bidder by MSLDC.
- ✓ Perform regular file archival and purge as necessary.
- ✓ Provide user support, as needed. Investigate and troubleshoot issues.
- ✓ Coordinate and communicate with respective CSP. Know how to implement and control the flow of data, to and from the CSP to MSLDC.

4. Annual Maintenance Services for Data Warehousing System

This Section covers the requirement of Annual Maintenance Services to be provided by the Bidder during Warranty Period and AMC period. The Proposed AMC services are indicative and Bidder shall provide all the necessary services during warranty and AMC period to maintain the Data Warehousing System and allied Software to the highest service level upto the satisfaction of MSLDC.

- **Annual Maintenance Services**

The warranty period shall be of 3 (Three) years from the date of successful completion and taking over of the project. The Annual Maintenance Contract (AMC) shall be for 3 (Three) years starting after the date of expiry of warranty period. The bidder shall provide full support in AMC for three years including the cloud services, if any, from the date of expiry of warranty period. The support will include

- ✓ 24x7 on line support i.e. internet connectivity shall be used for remote connectivity. Response time shall be 2 Hrs.
- ✓ Bidder shall deploy qualified technical resource having Minimum 3 - 5 years of experience on fulltime basis (Monday to Saturday) at MSLDC for the entire Warranty and AMC period.
- ✓ In case of critical problems bidder shall send his representative within 6 hours and he will ensure the restoration the normalcy within 12 hours from the receipt of complaint. The traveling, lodging etc. will be borne by the Bidder. Annual Maintenance Contract (AMC) price will be considered for evaluation of bid along with Development & Implementation price quoted.
- ✓ Bidder shall provide support and bug-fixed to the custom developed Data Warehousing System software application and its Application programming Interfaces (APIs) under the scope of work for this project.
- ✓ Overall monitoring of the deployed network bandwidth/ links so as to ensure the desired uptime. In case of downtime/ link failure, reporting immediately the same to the Network Bandwidth Provider (NBP) and tracking until the link is restored and services are operational as required.
- ✓ In the event of onsite deployed resource(s) leaving the project/ employment, the

same shall be immediately replaced with another resource of equivalent or higher qualifications and experience. All such events should be notified to the MSLDC well within time.

- ✓ At no time, the provided manpower should be on leave or absent from the duty without prior permission from the designated nodal officer of MSLDC. In case of long-term absence due to sickness, leave etc. the Solution Provider shall ensure replacements and manning of all manpower posts by without any additional liabilities to MSLDC. Substitute will have to be provided by the Solution Provider against the staff proceeding on leave/ or remaining absent and should be of equal or higher qualifications/ experience.
- ✓ Bidder is required to provide detailed profile of the team proposed during Warranty and AMC period in technical bid.
- ✓ Any bug reported / lack of compliance with requirement during Warranty & AMC Period, will be fixed free of cost by the vendor. Changes and bug fixes carried out during maintenance should be propagated to all the environments. Bidder should take necessary precautions to preserve existing data and MSLDC's functioning.
- ✓ You shall ensure the availability of Data ware housing system web application as per the SLA defined during contract period.
- ✓ You shall provide 24*7*365 support to ensure the availability of the Data ware housing system web application during entire Contract Period (Warranty Period + AMC Period).
- ✓ The bidder should provide 24*7 Helpdesk support, System Administration Support during entire Contract Period (Warranty Period + AMC Period) .
- ✓ Scope also includes, without any extra cost to MSLDC, installation/reinstallation of instances including OS, database, application etc, software updates for the OS, patches, bug fixes, resolving issued related to OS, Application, database, integration etc. and updating the security of the network during warranty / AMC period.
- ✓ You shall be responsible for Providing all software updates and patches released by the hardware OEM, update and patch management, resolution of any issues/problems with the hardware etc.
- ✓ Any required version/Software /Hardware upgrades, patch management etc. at the Cloud Site will be supported by the Bidder for the entire contract period as well as during AMC period at no extra cost to MSLDC.
- ✓ Time to time attend any specific problems reported by the client for the smooth functioning of the Data ware housing system web application.
- ✓ You shall perform preventive maintenance on monthly basis & submit the report to MSLDC.
- ✓ Bidder shall be responsible for ensuring security of Data ware housing system and infrastructure from any threats and vulnerabilities. You shall address ongoing needs of security management including, but not limited to, monitoring of various devices /tools such as firewall, intrusion prevention/ detection, content filtering and blocking, virus protection, even logging & correlation and vulnerability protection through implementation of proper patches and rules.
- ✓ Bidder shall be responsible for implementation of Cyber Security related advisories/alerts related to the Data ware housing system / cloud resources / services, received from CERT-In, CERT-GO, CERT-Trans, CSK, NCIIPC and other statutory agencies within the timelines stipulated by the agencies or MSLDC,

without any additional cost to MSLDC.

- ✓ You should comply with all the present and future provisions of the MSETCL Information Security Policy/NCIIPC Guidelines/Guidelines of CERT/CEA, Respective Govt. Agencies and provide such regulatory requirements at no additional cost to MSETCL during the contract period. The Systems may be audited by MSETCL/any other Regulatory Authority or Authority appointed by MSETCL and any observation pointed out (related to cloud resources / services) by these bodies have to be complied by the vendor within the timelines stipulated by the agencies or MSETCL, without any additional cost to MSETCL. Data ware housing system shall be subjected to Cyber Security Audit (including VAPT and functional/OS audit) at any time during the contract period. The auditors may be internal/ external. The vendor should provide solution and implementation for all the audit points (related to cloud resources / services) raised by MSETCL's internal/external team during the contract period, within the stipulated timelines, without any extra cost. Extreme care should be taken by the vendor to ensure that the observations do not get repeated in subsequent audits.
- ✓ Ensuring Uptime and utilization of the cloud resources as per SLA's defined in this tender document.

- **Preventive maintenance (On Monthly Basis) during Warranty and AMC Period**
  - ✓ The AMC engineer shall carry out following activities as per the pre-approved schedule
    - ➢ Check system errors, if any and determine the status / health of the Data Warehousing Web Application.
    - ➢ Carry out tests, if required, for the proper functioning of the software application.
    - ➢ Take back-up of database, software application before change request patches applied to the existing application.
    - ➢ Apply security patches of database, OS & other Software components, if any.
    - ➢ Restart the system, if required.
    - ➢ Application and Database cleanup activity including rebuilding indexes, Managing database, fine tuning of database for better performance etc
    - ➢ Database administration activities including performance tuning, System administration activities.
    - ➢ Backup of Application and Database and archiving.
    - ➢ Prepare and share an Inspection report to MSLDC.

  - ✓ In addition to the above, Bidder shall carry out the following activities:
    - ➢ Diagnose the system health
    - ➢ Restart the system including database, if required.
    - ➢ Re-configure the system including database, if required.
    - ➢ Initiate database backup
    - ➢ Any other activities as may be necessary

- **Break down maintenance (As and when required) during Warranty and AMC Period**
  - ✓ On receipt of call from MSLDC or its Authorized Representative, the AMC engineer shall carry out the following activities –
    - ➢ Check system errors and determine the status / health of the Data Warehousing Web Application.
    - ➢ Execute tests for proper functioning of the Data Warehousing Web Application including OS, database, web servers and disaster recovery.
    - ➢ Execute assessment to determine the current status and diagnose the cause of error (internal or external)
    - ➢ Take action to restore the system to working condition after putting necessary backup form the archive, if required.
    - ➢ In case of reinstallation/re-configuration of the system (OS, database or application Server components) is required, it will be done, Re-configure the system database, changes to configurations if required.
    - ➢ Prepare Fault Clearance Reports / Inspection reports jointly with MSLDC personnel.

  - ✓ In addition to the above, Bidder shall shall carry out the following activities:
    - ➢ Diagnose the system health
    - ➢ Restart the system including database, if required
    - ➢ Re-configure the system including database, if required.
    - ➢ Initiate database backup
    - ➢ Any other activities as may be necessary

5. Change Request

- Bugs, lacunae, non-compliance to specifications, discovered during or after the testing process cannot be treated as change request
- During **three-year free warranty** period, you shall be responsible to attend the change request up to 25-man days efforts free of cost.
- During AMC period (after end of **three-year free warranty** period), you shall be responsible to attend the change request up to 25-man days efforts free of cost, on yearly basis.
- Change request beyond the limit of **25-man days** efforts shall be on chargeable basis as per the quoted rates.
- Work Order for the Change request will be issued separately on the basis of quoted rates on pro-rate basis, for the actual Man Days required to complete the Change Request. Scope of Work, Terms & Conditions for the Work Order shall be as per the tender document.
- Bidder is supposed to hand over the complete, fully tested/ audited, bug free, final version of source code (in softcopy format) of **Data ware housing system** web application.

6. OS, Database & other applications Management

- You shall be responsible for maintenance of the Operating System, database and other associated tools/application required for smooth functioning of **Data ware housing**

system web application.

- You shall be responsible for installation/re-installation/configuration of the Operating System, Database or other application required for smooth functioning of **Data ware housing system** web application.
- You shall be responsible for security Patches/upgrade etc related to OS, Database & other applications being used for **Data ware housing system** web application.

7. Cyber Security Audit of Data ware housing system web application

- You shall be responsible for cyber security audit of the proposed Data ware housing system web application as per the guidelines specified by Indian Computer Emergency Response Team (CERT-In) / CEA. The security audit agency shall be an empanelled agency in CERT-In.
- You shall perform Cyber Security Audit of the proposed Data ware housing system web application before acceptance of the system i.e. before go-live.
- You shall perform Cyber Security Audit of the proposed Data ware housing system web application on bi-annually basis after go-live of the Data ware housing system web application during entire contract period i.e. (Warranty + AMC Period)
- All vulnerabilities identified during Cyber Security Audit shall be closed by you within a period of one month without any additional financial implications to MSLDC.
- After closure of the all vulnerabilities identified, Cyber security audit certificate shall be provided by the bidder from CERT-IN empanelled agency.

8. Security and Statutory Requirements

8.1 Privacy and Security Safeguards.

1. Bidder to ensure that the data is encrypted as part of a standard security process for highly sensitive content or choose the right cryptographic algorithms evaluating security, performance, and compliance requirements specific to their application and may choose from multiple key management options.
2. Bidder to notify the MSLDC promptly in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data, to enable the agency to manage these events proactively.
3. The Bidder shall ensure that all the storage blocks or multiple copies of data if any are unallocated or zeroed out by the CSPs so that data cannot be recovered. If due to some regulatory reasons if it is required to securely decommission data, departments can implement data encryption at rest using departments managed keys, which are not stored in the cloud. Then MSLDC may delete the key used to protect the decommissioned data, making it irrecoverable.
4. The Bidder shall report forthwith in writing of information security breaches to the MSLDC by unauthorized persons other than authorised by MSLDC (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential Information.
5. The Bidder undertakes to treat information passed on to them under this Agreement as classified. Such Information will not be communicated / published / advertised by the Bidder to any person/organization without the express permission of the MSLDC.

8.2 Confidentiality

1. The Bidder shall execute non-disclosure agreements with the MSLDC with respect to Data Warehousing Web Application project. For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:
    a. Information already available in the public domain;
    b. Information which has been developed independently by the Service Provider;
    c. Information which has been received from a third party who had the right to disclose the aforesaid information;
    d. Information which has been disclosed to the public pursuant to a court order.
2. The Bidder will be permitted to obtain data only to deliver the services to MSLDC under this project. Bidder shall not retain the data or use for any other purpose. The bidder remains responsible for all its subcontractors/ service provider's compliance with bidder's obligations under the Project.

8.3 Location of Data:

1. The location of the data (text, audio, video, image files, drawing files, GIS files, pdf, and any compressed data and software (including machine images), that are provided to the CSP for processing, storage or hosting by the CSP services in connection with the MSLDC account and any computational results that an MSLDC or any end user derives from the foregoing through their use of the CSP's services) shall be as per the terms and conditions of the Empanelment of the Cloud Service Provider.
2. Nature of replication between the DC and DRC (e.g., asynchronous replication of data between Primary DC and DRDC)
3. RPO should be less than or equal to <<30 Minutes>> and RTO shall be less than or equal to <<2 hours>>.
4. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site
5. In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. Application data and application states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO.

8.4 E-Discovery:

Electronic discovery (e-discovery) is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. MSLDC must be able to access and retrieve such data in a CSP environment in a timely fashion for normal work purposes.

8.5 Law Enforcement Request:

The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the Cloud Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency.

8.6 Audit:

MSLDC shall ensure that the Cloud Service Provider's services offerings are audited and certified by STQC/MeitY. MSLDC include the following clauses in the Agreement:

1. The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines as and when published).
2. The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service Provider.

8.7 Performance Management:

The critical SLAs for cloud services are covered under Annexure of this document

8.8 Audit and Governance Requirements

The CSP shall implement the audit & compliance features to enable the Agency to monitor the provisioned resources, performance, resource utilization, and security compliance:

1. View into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.
2. Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.
3. System-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources.
4. Review of auto-scaling rules and limits.
5. Logs of all user activity within an account. The recorded information should include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service. This is required to enable security analysis, resource change tracking, and compliance auditing.
6. Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered each time a configuration changes, and Agencies should be given the ability to dig into the configuration history to perform incident analysis.
7. Monitoring of cloud resources with alerts to customers on security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies.
8. Automated security assessment service that helps improve the security and compliance of applications deployed on cloud by automatically assessing applications for vulnerabilities or deviations from best practices. After performing an assessment, the tools should produce a detailed list of security findings prioritized by level of severity.

8.9 Exit Management / Transition-Out Responsibilities

1 Continuity and performance of the Services at all times including the duration of the Agreement and post expiry of the Agreement is a critical requirement of

MSLDC. It is the prime responsibility of Bidder to ensure continuity of service at all times of the Agreement including exit management period and in no way any facility/service shall be affected/degraded.

2. The responsibilities of Service Provider with respect to Exit Management /Transition-Out services on cloud include:

a. Provide a comprehensive exit management plan. Provide necessary handholding and transition support to ensure the continuity and performance of the Services to the complete satisfaction of MSLDC.
b. Support MSLDC in migration of the VMs, data, content and any other assets to the new environment created by MSLDC or any Agency (on behalf of MSLDC) on alternate cloud service provider's offerings to enable successful deployment and running of the MSLDC's solution on the new infrastructure by providing a mechanism to MSLDC for the bulk retrieval of all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to MSLDC supplied industry standard media.
c. The format of the data transmitted from the cloud service provider to MSLDC should leverage standard data formats (e.g., OVF, VHD…) whenever possible to ease and enhance portability. The format will be finalized by MSLDC.
d. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with MSLDC.
e. Ensure that all the documentation required by MSLDC for smooth transition including configuration documents are kept up to date and all such documentation is handed over to MSLDC during regular intervals as well as during the exit management process.
f. Shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of MSLDC.
g. Once the exit process is completed, remove the MSLDC's data, content and other assets from the cloud environment and certify that the VM, Content and data destruction to MSLDC as per stipulations and shall ensure that the data cannot be forensically recovered.
h. There shall not be any additional cost associated with the Exit / Transition- out process.

9. DOCUMENTATION REQUIREMENTS FOR CLOUD HOSTING

9.1 Introduction

Documentation of Cloud VM Instances, vCPUs, Storage, Hosting Location and DR Locations in cloud, Additional Services opted and any other Cloud related technical details deployed for the Data Warehousing Web Application system shall meet following documentation requirements. All documents shall be supplied in hard copies as well as soft copies:-

9.2 Design Documents

Before deployment of the Data Warehousing Web Application into the cloud, a detailed IT architecture shall be submitted by the CSP through Bidder.

The design document must essentially (but not limited to) included:-

- Cloud Instances/VMs, Storage, Additional Services Overview
- Cloud System configurations for VMs and Storages
- Cloud Architecture diagram for Data Warehousing Web Application integration with MSLDC
- Physical details of each Cloud component
- Overall Cloud networking scheme

9.3 User Manuals

Following user manuals shall be prepared and supplied for the system:-

9.3.1 User Manual for MSLDC

User manual for MSLDC personnel should contains all user instructions, block diagrams, user screens etc. in order to make itself contain complete document required for operation of complete Data Warehousing Web Application and its integration with existing software applications from the Cloud to the MSLDC Data Centre.

9.3.2 Training Documents

Training document to be used during training of state entity personals shall contain major functional details of the overall Data Warehousing Web Application, its features and major instructions for understanding the overall working of the system. Technical review & documentation should cover all technical aspects in details.

TERMS and CONDITIONS:

1) **Warranty Period:** All the deliverables, products and services given to MSLDC within the scope of this work shall have a warranty period of **three** year. The warranty period shall start, after of completion of the hyper care period & it is certified by MSLDC. After the expiry of the warranty period, the service need not be continued taking it as deemed extension of period.
2) **Payment Schedule:**

A. Development of the Data ware housing system

Following Table provides the activity wise payment schedule for Development of the Data ware housing system

Sr. No.	Milestone	Payment
1		
2		
3		

Bidder should submit invoice in triplicate along with deliverables after completing the milestone, and payment will be made within 45 days subject to availability of fund. Such invoices should accompany the deliverables

B. Hosting of the Data ware housing system on cloud

a. Payment (for all types of Cloud Services) will only start after successful completion of the Hypercare period and after producing certificate from MSLDC in that regard.
b. Payment to be linked to the compliance with the SLA metrics and the actual payment is the payment due to the Service Provider after any SLA related deductions if any.
c. The income tax (TDS) will be deducted from the payment / amount credited prevailing rates if applicable
d. Bidder should submit invoice in triplicate at the end of every quarter and payment will be made within 45 days subject to availability of fund. Such invoices should accompany
    i. Cloud VM resource utilization report.
    ii. Data ware housing system and Cloud resource Availability Report
    iii. Consolidated SLA report duly certified by MSLDC Engineer
    iv. Valid STQC audit compliance and Meity empanelment letter
    v. Compliance report for implementation of advisories/alerts received from CERT-In, CERT-GO, CERT-Trans, CSK, NCIIPC and other statutory agencies and compliance of Observations/recommendations of Cyber Security Audit (VAPT) of Data ware housing system, if any.

C. Cyber Security Audit of **Data ware housing system**

a. The income tax (TDS) will be deducted from the payment / amount credited prevailing rates if applicable
b. Payment will be affected to you within 45 days subject to availability of fund, on submission of the invoice in triplicate along with
    i. Cyber Security Audit Observations report
    ii. Cyber Security Audit Certificate

3) **Penalty (Liquidated Damages (LD)):** If the contractor fails to complete the work within stipulated period of ----- weeks from the date of issue of LOA / Work Order, penalty towards delay @ ½ % per week of the invoice value, maximum extent of 10% of order value, will be levied and deducted from bill for non-execution of work. For the purpose of penalty clause, the completion of works in all respects to the satisfaction of the MSLDC shall be considered to be applicable.

4) Penalties:

A. Web Application Maintenance Services:

- Bidder shall provide immediate maintenance support and assistance in the event of any disruption to the Web Application. The manner and time frame for troubleshooting and the timelines for the resolution of the problems will be as follows:

Priority	Priority Definition	Resolution Time	Penalty
High	Out of Service – Web Application is not functioning	As per **Annexure 'D'**	As per **Annexure 'D'**
Medium	• Defects in the Web Application functionality • Web Application is not functioning as intended • Any other issues as per the Scope of Work	4 Hours	1 % of Monthly Payment of Cloud hosting Services per day.
Low	All other requests, Any other minor issues not affecting performance & functionality of the Web Application.	24 Hours	0.5 % of Monthly Payment of Cloud hosting Services per day.

B. Cloud Services:

- Payments to the Bidder for the provided Services to be linked to the compliance with the Service Level Agreement (**Annexure – D**)
- The penalty in percentage of the <<Periodic Payment>>) is indicated against each SLA parameter in the table in **Annexure-D**.
- If the penalties are to be levied in more than one SLA then the total applicable penalties are calculated and deducted from the total of the <<periodic/monthly> bill and the balance paid to the SP.
  e.g.: SLA1 =7% of the <<Periodic Payment (monthly)>>, SLA12=10% of the <<Periodic Payment (monthly)>>, SLA19=2% of the <<Periodic Payment (monthly)>> then
  Amount to be paid = Total <<periodic/monthly> bill - {(19% of the <<Periodic Payment (monthly)>>)}
- In case multiple SLA violations occur due to the same root cause or incident then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a sum of penalties for the applicable SLA violations
- Penalties shall not exceed 100% of the <<periodic/monthly>> bill. If the penalties exceed more than 50% of the total <<periodic/monthly> bill, it will result in a material breach. In case of a material breach, the operator will be given a cure period of one month to rectify the breach failing which a notice to terminate may be issued by the MSLDC

5) All the data created as the part of the project shall be owned by MSLDC. The Bidder shall take utmost care in maintaining security, confidentiality and backup of this data. MSLDC shall retain ownership of any user created/loaded data and applications hosted on Bidder's /CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time. Bidder shall have to sign a Non-Disclosure Agreement as per the format of Annexure 'E' with MSLDC within 7 (Seven) days from the date of receipt of Letter of Award/Work Order.

6) **Patent Rights & Royalties:**

- Royalties and fees for patents covering materials, articles, apparatus, devices, equipment or processes used in the Works shall be deemed to have been included in the Contract Price. The Contractor shall satisfy all demands that may be made at any time for such royalties or fees and he alone shall be liable for any damages or claims for patent infringements and shall keep the Owner indemnified in that regard. The Contractor shall, at his own cost and expenses, defend all suits or proceedings that may be instituted for alleged infringement of any patents involved in the works and in case of an award of damages, the Contractor shall pay for such award. In the event of any suit or other proceedings instituted against the Owner, the same shall be defended at the cost and expenses of the Contractor who shall also satisfy/comply the decree, order or award made against the Owner. Final payment to the Contractor by the Owner will not be made while any such suit or claim remains unsettled. In the event any apparatus or equipment or any part thereof furnished by the Contractor is in such suit or proceedings held to constitute infringement, and its use is enjoined, the Contractor shall, at his option and at his own expense, either procure for the Owner the right to continue use of said apparatus, equipment or part thereof, replace it with non-infringing apparatus or equipment or modify it, so that it becomes non-infringing.

- The Contractor shall be responsible for the observance by his sub-contractors of the foregoing.

7) Post completion of the Warranty Period, Successful bidder shall be bound to accept the Work Order for AMC of the web application & Change request for web application on the quoted rates by bidder. Scope of Work and the terms & conditions shall be as per this tender document.

8) Work Order for AMC of Web Application shall be issued to the successful bidder on annual basis, post completion of the warranty period.

9) In case MSLDC has the requirement for Change Request for web application, Work Order for change request shall be issued by MSLDC for the period of man-days required for completion of the change request. Rates quoted by the bidder on pro-rate basis shall be considered for issuance of this work order.

Annexure –'A'
Technical Specification

Sr. no	SKU Name	Product Description	Minimum Qty
Preferred CSP : Amazon (AWS) / Microsoft (Azure) / Google (GCP) / Oracle (OCI)			
DC			
Production			
1	Application Server in HA(RHEL)	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
2	Database Server in HA (RHEL)	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
3	Additional Storage	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
4	Internet Data Transfer on 1 Gbps Port	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	-
5	Public IP of IPv4	Static Public IP of IPv4	1
6	SSL Certificate	SSL Certificate for production application servers	1
7	WAF	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
8	Load Balancer for App / DB	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
9	DDOS Service	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
UAT			
1	Application and Database Server	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
2	Additional Storage	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
3	INTERNET DATA TRANSFER on 1 Gbps Port	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	-
Other			
1	RHEL Support Subscription	Monthly Support Subscription for Red Hat Enterprise Linux for all the Virtual Machines	1
2	BACKUP LICENSE &	Capacity Based Backup License / Applicable for Servers/ VM snapshot backup, file/folder backup, database backup, application	

	STORAGE	backup. Note: Backup of the all Virtual Machines infrastructure is required. License & storage shall be calculated accordingly.	1
3	Firewall	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
4	VPN	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
Disaster Recovery			
1	Application Server (RHEL)	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
2	Database Server (RHEL)	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
3	Additional Storage	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
4	Public IP of IPv4	Static Public IP of IPv4	2
5	INTERNET DATA TRANSFER on 1 Gbps Port	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	-
6	RHEL Support Subscription	Monthly Support Subscription for Red Hat Enterprise Linux for DR Virtual Machines	1
7	BACKUP LICENSE & STORAGE	Capacity Based Backup License | Applicable for Servers/ VM snapshot backup, file/folder backup, database backup, application backup. Note : Backup of the all Virtual Machines deployed for Data Warehousing Web Application at DR Site is to be taken. License & storage shall be calculated accordingly.	1
8	Firewall	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
9	SSL Certificate	SSL Certificate for application servers	1
10	WAF	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1
11	VPN	<< Detailed technical specification to be filled by the bidder considering the scope of work>>	1

Annexure –'B'

Services

Service	Sr. No.	Replication Management
Replication Management	1	Replication Configuration
	2	Replication Monitoring
	3	Troubleshooting replication issues
	4	Failover/ Failback
	5	DR Drill (Six Monthly)
	6	DR Drill Reports
Cloud Managed Services	1	OS Management and administration
	2	OS installation and configuration for monitoring and ITSM tool.
	3	Local user and group management (create / modify / delete)
	4	OS hardening.
	5	OS Patch Management as per policy.
	6	Memory and hardware configuration.
	7	Incident management, handling service requests, problem management, change management
	8	Response to alert generated by system or problem reported by client.
	9	Troubleshooting, root cause analysis, problem identification and resolution.
	10	Fully managed database service. DBA Service.
Network and Security Management	1	Change Security Groups associated with the instances.
	2	Start/Stop/Terminate an instance.
	3	Provisioning IP addresses for instances as per architecture.
	4	Associating and de-associating IP addresses with instances.
	5	Checking the Firewall settings of the instances.
	6	Update the existing Security Group.
	7	Creating, updating and deleting NACL (Network Access Control Lists).
	8	Creating, updating and deleting route table.
	9	Attaching and detaching a network interface.
	10	Manage Private IP Address.
	11	Creation of Network Interfaces.
	12	Creating a Security Group.
	13	Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized
	14	Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any
	15	Managing NAT gateway.
	16	Managing VPN Gateway server.

Annexure – 'C'

Price Schedule

Sr. No.	Description	Qty	Before Go-Live	After GO-Live					
			Rates	1st Year Rates	2nd Year Rates	3rd Year Rates	4th Year Rates	5th Year Rates	6th Year Rates
1	Development of **Data Warehousing System** web application as per scope of work.	Lump sum		NA	NA	NA	NA	NA	NA
2	Hosting of the **Data ware housing system** (As per Scope of Work) (***Preferred CSP:*** *Amazon (AWS) / Microsoft (Azure) / Google (GCP) / Oracle (OCI)*) For Warranty Period : < Years > And For AMC Period : < Years>		NA	NA	NA	NA	NA	NA	NA
	a) DC (Production)	Lump sum	NA						
	b) DC (UAT)	Lump sum	NA						
	c) DC (Other)	Lump sum	NA						
	d) DR	Lump sum	NA						
3	Database Licensing Cost (Oracle Standard Edition/Postgre Enterprise/MySql Enterprise (Latest Version) for Database Servers specified in Annexure 'A'	Lump sum	NA						
4	Third Party tool license for DC-DR sync. Or Any other license (If Applicable)	Lump sum	NA						
5	DBA Services	Lump sum	NA						
6	Cyber Security Audit of **Data Warehousing system** web application (As per Scope of Work) (Bi-Annually)	Lump sum							
7	BI and Data Analytics Tool	Lump sum	NA						
8	Annual Maintenance (AMC)	Lump sum	NA	NA	NA	NA			
9	Change Request Man days rate	Lump sum	NA						
		Sub Total							
		GST@ _____%							
		Total							
		Final Total							

Annexure – D

Cloud Service Level Agreement

Certain requirements are not mentioned in the SLAs, but Bidder / CSPs / MSPs are required to comply with the requirements mentioned in the empanelment RFP.

1. Measurement and Monitoring

a) The SLA parameters shall be monitored on a quarterly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of MSLDC, then the MSLDC will have the right to take appropriate disciplinary actions including termination of the contract.

b) The full set of service level reports should be available to the MSLDC on a monthly basis or based on the project requirements.

c) The Monitoring Tools shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. Bidder / CSPs / MSPs shall make available the Monitoring tools for measuring and monitoring the SLAs. Bidder / CSPs / MSPs may deploy additional tools and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. The tools should generate the SLA Monitoring report in the end of every month which is to be shared with the MSLDC on a monthly basis. The MSLDC shall have full access to the Monitoring Tools/portal (and any other tools / solutions deployed for SLA measurement and monitoring) to extract data (raw, intermediate as well as reports) as required during the project. The MSLDC will also audit the tool and the scripts on a regular basis.

d) The measurement methodology / criteria / logic will be reviewed by the MSLDC.

e) In case of default on any of the service level metric, the Bidder/CSP shall submit performance improvement plan along with the root cause analysis for the Department's approval.

2. Periodic Reviews

a) During the contract period, it is envisaged that there could be changes to the SLA, in terms of measurement methodology / logic / criteria, addition, alteration or deletion of certain parameters, based on mutual consent of both the parties, i.e. the MSLDC and Bidder.

b) MSLDC and Bidder shall each ensure that the range of the Services under the SLA shall not be varied, reduced or increased except by the prior written agreement of the MSLDC and Bidder in accordance with the Change Control Schedule.

c) The SLAs may be reviewed on an annual basis by the MSLDC in consultation with the Service Provider and other agencies.

d) All the SLA penalty calculation should be done for the mentioned calendar month.

3. Penalty Calculation

Payments to the Bidder for cloud services to be linked to the compliance with the SLA metrics laid down in this annexure.

a) The payment will be linked to the compliance with the SLA metrics

b) The penalty in percentage of the Quarterly Payment is indicated against each SLA parameter

c) The Service provider will be exempted from any delays or slippages on SLA parameters arising out of following reasons:-

I. The non-compliance to the SLA other than for reasons beyond the control of the Bidder / CSP / MSP. Any such delays will be notified in writing to the department and will not be treated as breach of SLA from the Bidder / CSP /MSP's point of view.

II. There is a force majeure event effecting the SLA which is beyond the control of the bidder / CSP.

d) The maximum penalty at any point of time on an additive basis in any quarter shall not exceed 50% of quarterly payments, it will result in a material breach. In case of a material breach, the bidder will be given a cure period of one month to rectify the breach failing which a notice to terminate may be issued by the MSLDC.

1. Service Levels

S.No#	Service Level Objective	Definition	Target	Penalty
Availability				
1	Availability of each cloud service (Applicable for all Cloud Service as defined in Cloud Services Bouquet)	Availability means, the aggregate number of hours in a calendar month during which cloud service is actually available for use through command line interface, user/admin portal and APIs (which ever applicable) Uptime Calculation for the calendar month: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability for each of the cloud service>=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 10% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 15% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 20% of Quarterly Payment of the Project d) <98% - 30% of the Quarterly Payment of the Project In case the services is not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the Quarterly Payment of the Project.

2	Availability of Critical Services(As defined in Annexure B) *This SLA shall not be applicable when the associated cloud service as mentioned in SLA#1 above is not available /Up.	Availability means, the aggregate number of hours in any specified time period during which the critical service is actually available for use through command line interface, user/admin portal and APIs (which ever applicable) Uptime Calculation for the calendar month: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability for each of the critical service>=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 5% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 10% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 15% of Quarterly Payment of the Project d) <98% - 20% of the Quarterly Payment of the Project In case the services is not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the Quarterly Payment of the Project.
3	Availability of regular reports (SLA, RCA, Cloud Services Consumption, Monitoring, Billing and Invoicing, Security, & Project Progress)	Regular reports should be submitted to the Government dept. within 5 working days from the end of the month.	Regular reports should be submitted to the Government dept. within 5 working days from the end of the month.	Penalty as indicated below (per occurrence): a) <11 working days to >= 6 working days - 2% of Quarterly Payment for the Project b) <16 working days to >= 11 working days - 4% of Quarterly Payment for the Project c) For the delay beyond 15 days , penalty of 5% of the Quarterly Payment for the Project

4	Availability of the Cloud Management Portal of CSPs	Availability means the aggregate number of hours in a calendar month during which cloud management portal of CSP is actually available for use Uptime Calculation for the calendar month: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x 100}	Availability of the Cloud Management Portal of CSP >=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 10% of Quarterly Payment of the Project b) <99.00% to >= 98.50% - 15% of Quarterly Payment of the Project c) <98.50% to >= 98.00% - 20% of Quarterly Payment of the Project d) <98% - 30% of the Quarterly Payment of the Project In case the Cloud Management Portal of the CSP is not available for a continuous period of 8 Business Hours on any day, penalty shall be 50% of the Quarterly Payment of the Project.

Security				
5	Percentage of timely vulnerability reports	Percentage of timely vulnerability reports shared by CSP/MSP with MSLDC within 5 working days of vulnerability identification. Measurement period is calendar month.	Percentage of timely vulnerability reports shared with MSLDC within 5 working days of vulnerability identification>= 99.95%	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of Quarterly Payment for the Project b) <99.00% to >= 98.00% - 20% of Quarterly Payment for the Project b) <98% - 30% of Quarterly Payment for the Project
6	Percentage of timely vulnerability corrections	Percentage of timely vulnerability corrections performed by CSP/MSP. a) High Severity - Perform vulnerability correction within 30 days of vulnerability identification. b) Medium Severity - Perform vulnerability correction within 60 days of vulnerability identification. c) Low Severity - Perform vulnerability correction within 90 days of vulnerability identification. Measurement period is calendar month.	Maintain 99.95% service level	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of Quarterly Payment for the Project b) <99.00% to >= 98.00% - 20% of Quarterly Payment for the Project b) <98% - 30% of Quarterly Payment for the Project

7	Security breach including Data Theft/Loss/Corruption	Any incident wherein system including all cloud-based services and components are compromised or any case wherein data theft occurs (includes incidents pertaining to CSPs only)	No breach	For each breach/data theft, penalty will be levied as per following criteria. 1. Severity 1 (as define in Annexure A) - Penalty of Rs 15 Lakh per incident. 2. Severity 2 (as define in Annexure A) - Penalty of Rs 10 Lakh per incident. 3. Severity 3 (as define in Annexure A) - Penalty of Rs 5 Lakh per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, << Government Department / Agency>> reserves the right to terminate the contract.
8	Security Incident (Malware Attack/ Denial of Service Attack/ Data Theft/ Loss of data/ Intrusion or Defacement) Applicable on the CSP's underlying infrastructure	Security incidents could consist of any of the following: Malware Attack: This shall include Malicious code infection of any of the resources, including physical and virtual infrastructure and applications. Denial of Service Attack: This shall include non-availability of	a) Any Denial-of-service attack shall not lead to complete service non-availability. b) Zero Malware attack / Denial of Service attack / Intrusion / Data Theft	For each occurrence of any of the attacks (Malware attack / Denial of Service attack / Intrusion / Data Theft), 10% of the Quarterly Payment of the Project

		any of the Cloud Service due to attacks that consume related resources. The Service Provider shall be responsible for monitoring, detecting and resolving all Denial of Service (DoS) attacks. Intrusion: Successful unauthorized access to system, resulting in loss of confidentiality/ Integrity/availability of data. The Service Provider shall be responsible for monitoring, detecting and resolving all security related intrusions on the network using an Intrusion Prevention device.		
Support Channels - Incident and Helpdesk				
9	Response Time under Enterprise Support (As defined under cloud service bouquet)	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 15 minutes	a) <95% to >= 90.00% - 5% of Quarterly Payment of Enterprise Support service b) <90% to >= 85.00% - 7% of Quarterly Payment of Enterprise Support service c) <85% to >= 80.00% - 9% of Quarterly Payment of Enterprise Support service d) Subsequently, for every 5% drop in SLA criteria - 2% of Quarterly Payment of Enterprise Support service

10	Percentage of timely incident report under Enterprise Support service (As defined under cloud service bouquet)	The defined incidents to the cloud service which are reported to the Government Dept. in a timely fashion. This is represented as a percentage by the number of defined incidents reported within 1 hr. after discovery in a month, over the total number of defined incidents to the cloud service which are reported within the month	95% of the incidents should be reported to Government Dept. within 15 min of occurrence.	a) <95% to >= 90.00% - 5% of Quarterly Payment of Enterprise Support service b) <90% to >= 85.00% - 10% of Quarterly Payment of Enterprise Support service c) <85% to >= 80.00% - 15% of Quarterly Payment of Enterprise Support service d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of Enterprise Support service

11	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 95% of the incidents should be resolved within 30 minutes of problem reporting	a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.00% - 10% of Quarterly Payment of the Project c) <85% to >= 80.00% - 15% of Quarterly Payment of the Project d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of the Project
12	Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting AND 95% of Severity 3 within 16 hours of problem reporting	a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.00% - 10% of Quarterly Payment of the Project c) <85% to >= 80.00% - 15% of Quarterly Payment of the Project d) Subsequently, for every 5% drop in SLA criteria - 5% of Quarterly Payment of the Project
Disaster Recovery and Data Backup Management				
13	Recovery Time Objective (RTO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RTO <= 4 hours	10% of Quarterly Payment of the Project per every additional 2 (two) hours of downtime
14	RPO (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RPO <= 2 hours	10% of Quarterly Payment of the Project per every additional 2 (two) hours of data loss

15	DR Drills	At least two DR drills in a year (once every six months) or as per the agreement	At least two DR drills in a year (once every six months) or as per the agreement	a) No of DR Drills =1 - 1% of the Yearly Payment of the Project b) No of DR Drills = 0 - 2% of the Yearly Payment of the Project These will be measured every six months and the liquidated damage will be levied at the end of year
16	Data Migration	Migration of data from the source to destination system	Error rate < .25%	a) Error Rate > 0.25% & <=0.30% - 1% of the Quarterly Payment of the Project b) Error Rate > 0.30% & <=0.35% - 2% of the Quarterly Payment of the Project c) Error Rate > 0.35% & <=0.40% - 3% of the Quarterly Payment of the Project For each additional drop of 0.05% in Error rate after 0.40%, 1% of Total Quarterly Payment of the Project will be levied as additional liquidity damage
Audit & Monitoring				
17	Patch Application	Patch Application and updates to underlying infrastructure and cloud service Measurement shall be done by analyzing security audit reports	95% within 8 Hrs. of the notification	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 5% of Quarterly Payment of the Project b) <90% to >= 85.0% - 10% of Quarterly Payment of the Project c) <85% to >= 80.0% - 15% of Quarterly Payment of the Project d) <80% - 20% of the Quarterly

				Payment of that Project
18	Audit of the Sustenance of Certifications	No certification (including security related certifications mandated under MeitY empanelment such as ISO27001, ISO27017, ISO27018, ISO20001 etc.) should lapse within the Project duration. Service Provider should ensure the sustenance / renewal of the certificates	All certificates should be valid during the Project duration	Delay in sustenance of certifications a) > 1 day & <= 5 days - 1% of the Quarterly Payment of the Project b) > 5 day & <= 15 days - 2% of the Quarterly Payment of the Project c) > 15 day & <= 30 days - 5% of the Quarterly Payment of the Project d) > 30 days, 10% of the Quarterly Payment of the Project
19	Non-closure of audit observations	No observation to be repeated in the next audit	All audit observations to be closed within defined timelines	Penalty for percentage of audit observations repeated in the next audit a) > 0 % & <= 10% - 5% of the Quarterly Payment of the Project b) > 10 % & <= 20% - 10% of the Quarterly Payment of the Project c) > 20 % & <= 30% - 20% of the Quarterly Payment of the Project d) >30% - 30% of the Quarterly Payment of the Project

Severity Levels

Severity Level	Description	Examples
Severity 1	Environment is down or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available	• Non-availability of VM. • No access to Storage, software or application
Severity 2	Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.	• Intermittent network connectivity
Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.	

Definitions

I. **Critical Services:** Critical service may be defined as Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / De-Activation; User Profile Management; Security Components, etc.

II. **Business Hours**: Business hours may be referred as prime business period, which shall be from 08:00 A.M IST till 10:00 PM IST on all days.

ANNEXURE -E

NON-DISCLOSURE AGREEMENT

[To be submitted on duly notarized stamp paper of INR 500]

Date:

This Declaration ("Declaration") is entered into as of _____
(the "Effective Date") by and between:

Disclosing Party: **Maharashtra State Load Despatch Center (MSLDC), Airoli. (MSETCL)**

And

Receiving Party: **M/s.** _____, as a(n) (Check one)

☐ Individual ☐ Corporation ☐ Limited Liability Company ☐ Partnership

☐ Limited Partnership ☐ Limited Liability Partnership ("Receiving Party")

Disclosing Party and Receiving Party have entered into a business relationship relating to:
_____
_____ (the "Transaction").

In connection with its respective evaluation of the Transaction, each party, their respective affiliates and their respective directors, officers, employees, agents or advisors (collectively, "Representatives") may provide or gain access to certain confidential and proprietary information. A party disclosing its Confidential Information to the other party is hereafter referred to as a "Disclosing Party." A party receiving the Confidential Information of a Disclosing Party is hereafter referred to as a "Receiving Party." In consideration for being furnished Confidential Information, Disclosing Party and Receiving Party agree as follows:

1. Confidential Information. Confidential information is:

☐ All information shared by Disclosing Party : "Confidential Information" shall mean (i) all information relating to Disclosing Party's products, business and operations including, but not limited to, financial documents and plans, customers, suppliers, manufacturing partners, marketing strategies, vendors, products, product development plans, technical product data, product samples, costs, sources, strategies, operations procedures, proprietary concepts, inventions, sales leads, sales data, customer lists, customer profiles, technical advice or knowledge, contractual agreements, price lists, supplier lists, sales estimates, product specifications, trade secrets, distribution methods, inventories, marketing strategies, source code, software, algorithms, data, drawings or schematics, blueprints, computer programs and systems and know-how or other intellectual property of Disclosing Party and its affiliates that may be at any time furnished, communicated or delivered by Disclosing Party to Receiving Party, whether in oral, tangible, electronic or other form; (ii) the terms of any agreement, including this Agreement, and the discussions, negotiations and proposals related to any agreement; (iii) information acquired during any tours of Disclosing Party's facilities; and (iv) all other non-public information provided by Disclosing Party whosoever. All Confidential Information shall remain the property of Disclosing Party.

2. Exclusions from Confidential Information: The obligation of confidentiality with respect to Confidential Information will be approved by CISO of disclosing Party only after providing proper

justification.

3. Obligation to Maintain Confidentiality With respect to Confidential Information:

a. Receiving Party and its Representatives agree to retain the Confidential Information of the Disclosing Party in strict confidence, to protect the security, integrity and confidentiality of such information and to not permit unauthorized access to or unauthorized use, disclosure, publication or dissemination of Confidential Information except in conformity with this Agreement.

b. Receiving Party and its Representatives shall adopt and/or maintain security processes and procedures to safeguard the confidentiality of all Confidential Information received by Disclosing Party using a reasonable degree of care, but not less than that degree of care used in safeguarding its own similar information or material.

c. Upon the termination of this Agreement, Receiving Party will ensure that all documents, memoranda, notes and other writings or electronic records prepared by it that include or reflect any Confidential Information are returned or destroyed as directed by Disclosing Party.

d. If there is an unauthorized disclosure or loss of any of the Confidential Information by Receiving Party or any of its Representatives, Receiving Party will promptly, at its own expense, notify Disclosing Party in writing and take all actions as may be necessary or reasonably requested by Disclosing Party to minimize any damage to the Disclosing Party or a third party as a result of the disclosure or loss; and

e. The obligation not to disclose Confidential Information shall: (Check one)

☐ Survive the termination of this Agreement, and at no time will Receiving Party or any of its Representatives be permitted to disclose Confidential Information, except to the extent that such Confidential Information is excluded from the obligations of confidentiality under this Agreement pursuant to Paragraph 2 above.

☐ Remain in effect until termination of contract of _____ or until the Confidential Information ceases to be a trade secret, except to the extent that such Confidential Information is excluded from the obligations of confidentiality under this Agreement pursuant to Paragraph 2 above.

4. Non-Disclosure of Transaction : Without Disclosing Party's prior written consent, neither Receiving Party nor its Representatives shall disclose to any other person, except to the extent, the provisions of Paragraph 2 apply.

5. Representatives : Receiving Party will take reasonable steps to ensure that its Representatives adhere to the terms of this Agreement. Receiving Party will be responsible for any breach of this Agreement by any of its Representatives.

6. Disclaimer : There is no representation or warranty, express or implied, made by Disclosing Party as to the accuracy or completeness of any of its Confidential Information. Except for the matters set forth in this Agreement, neither party will be under any obligation with regard to the Transaction. Either party may, in its sole discretion: (a) reject any proposals made by the other party or its Representatives with respect to the Transaction; (b) terminate discussions and negotiations with the other party or its Representatives at any time and for any reason or for no reason; and (c) change the procedures relating to the consideration of the Transaction at any time without prior notice to the other party.

7. Remedies : Each party agrees that use or disclosure of any Confidential Information in a manner inconsistent with this Agreement will give rise to irreparable injury for which: (a) money damages may not be a sufficient remedy for any breach of this Agreement by such party; (b) the

other party may be entitled to specific performance and injunction and other equitable relief with respect to any such breach; (c) such remedies will not be the exclusive remedies for any such breach, but will be in addition to all other remedies available at law or in equity; and (d) in the event of litigation relating to this Agreement, if a court of competent jurisdiction determines in a final non-appealable order that one party, or any of its Representatives, has breached this Agreement, such party will be liable for reasonable legal fees and expenses incurred by the other party in connection with such litigation, including, but not limited to, any appeals.

8. Jurisdiction : Any dispute arises in between the parties, then jurisdiction of the Court shall be at Mumbai only.

9. Notices : All notices given under this Agreement must be in writing. A notice is effective upon receipt and shall be sent via one of the following methods: delivery in person, overnight courier service, certified or registered mail, postage prepaid, return receipt requested, addressed to the party to be notified at their address or by facsimile at the respective contact number or in the case of either party, to such other party, address or facsimile number as such party may designate upon reasonable notice to the other party.

10. Miscellaneous : This Agreement will inure to the benefit of and be binding on the respective successors and permitted assigns of the parties. Neither party may assign its rights or delegate its duties under this Agreement without the other party's prior written consent. Any provision of this Agreement shall not be affected and shall continue to be valid, legal and enforceable as though the invalid, illegal or unenforceable parts had not been included in this Agreement. Neither party will be charged with any waiver of any provision of this Agreement, unless such waiver is evidenced by a writing signed by the party and any such waiver will be limited to the terms of such writing.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date first written above.

Disclosing Party: **Maharashtra State Load Despatch Center (MSLDC), Airoli (MSETCL).**

Disclosing Party Representative Signature:

Disclosing Party Representative Full Name:

Receiving Party: : **M/s. _____**

Receiving Party and Representative Seal/Signature:

Receiving Party and Representative Full Name:

ANNEXURE -F

Guidelines to improve Cyber Security Posture

1. **Application Programming Interface (API) Security**

- Bidder shall ensure the activities and tasks associated with application programming interface security outlined as below
  - Secure Development Practices
  - Embed security in the software development lifecycle by using tools for static and dynamic code analysis.
  - Conduct regular code reviews with a focus on security.
  - Ensure developers are trained in and adhere to secure coding guidelines.
  - Authentication and Authorization Standards
  - Implement industry-standard authentication and authorization mechanisms.
  - Enforce the principle of least privilege for API access.
  - Regularly audit and update access control policies.
  - Data Protection
  - Enforce encryption of data in transit (using TLS) and at rest.
  - Mask or redact sensitive data exposed in API responses.
  - Securely manage API keys and tokens.
  - Threat Modelling and Testing
  - Perform threat modelling in the design phase to identify and address potential security issues.
  - Conduct penetration testing to simulate attacks and identify vulnerabilities before production deployment.
  - API Gateway Configuration
  - Configure an API gateway for rate limiting, IP filtering, logging, and to serve as a security policy enforcement point.
  - Patching and Updating
  - Keep the API Servers and Gateways updated with the latest security patches to protect against known vulnerabilities.
  - Ensure that any antiquated encryption algorithms and protocols are deprecated from the environment associated with API.
  - Incident Response Preparedness
  - Develop an incident response plan specific to API-related breaches.
  - Regularly conduct drills to ensure the team is prepared to manage and mitigate security incidents.
  - Monitoring and Regular Audits
  - Monitor API traffic for unusual patterns that may indicate a security threat.
  - Carry out regular API security assessments.
  - Conduct regular security audits to ensure compliance with internal and external regulations.

- Governance Guidelines
  - Identify and document all internal and external APIs in use.
  - Conduct a risk assessment for each API to understand the potential threats and vulnerabilities associated with its use and to implement the appropriate level of security controls.

- Technical Guidelines
  - Bidder should secure the API server environment, including the host operating system and the network
  - Bidder should ensure proper authentication and authorization controls are in place, such as

OAuth or API keys, to manage access to API functionalities securely.

- Bidder should follow the best practices for API key management as given below,
  - ✓ Generate API keys using strong, random algorithms to ensure they are unique and hard to guess.
  - ✓ Use long and complex API keys to increase security.
  - ✓ Encrypt API keys both at rest and in transit using strong encryption algorithms.
  - ✓ Assign API keys the minimum permissions necessary for their intended use.
  - ✓ Regularly rotate API keys to limit the exposure of keys that may be compromised.
  - ✓ Enable logging of all API key activities, including creation, usage, rotation, and revocation, and regularly review logs for anomalies.
  - ✓ Restrict API key usage to specific IP addresses or ranges to limit access to known and trusted sources.
  - ✓ Apply restrictions on API key usage based on criteria such as time of day, number of requests, and specific endpoints.
  - ✓ Use separate API keys for development, testing, and production environments to reduce the risk of accidental exposure and misuse.
  - ✓ Configure API keys with expiration dates to limit their validity period and reduce the risk of long-term exposure.
  - ✓ Implement rate limiting on API key usage to protect against abuse and denial-of-service attacks.
  - ✓ API keys should not be directly embedded in the code as exposure/sharing of the code without removing the keys may lead to accidental exposure of the keys.
  - ✓ API keys should not be stored in files inside the application's source tree.
  - ✓ API keys should be regenerated periodically, and applications should be updated to use the newly generated keys. Sdsad
  - ✓ level of security controls.
- Bidder should minimize data collection and storage to only what is necessary. Integrate privacy considerations from the initial stages of API development and perform a Privacy Impact Assessment (PIA) to identify and mitigate potential privacy risks.
- Bidder shall maintain an inventory of API dependencies and regularly update libraries and frameworks to patch known vulnerabilities
- Bidder shall ensure to implement API security parameters for input validation to protect against SQL injection, cross-site scripting (XSS), and other injection attacks.
- Bidder must use secure communication protocols, such as TLS, to encrypt data in transit between the client and the API to prevent eavesdropping and man-in-the-middle attacks. CSE shall employ rate limiting and throttling mechanisms to protect APIs from abuse and denial-of-service attacks.
- Bidder shall use API gateways or service meshes to enforce policies, for centralized security enforcement, monitoring, and management.
- Bidder must implement logging and monitoring strategies to detect and respond to suspicious API activities in real time.

- Bidder must monitor and regularly review API activity logs for tracking usage patterns and detecting anomalous behavior that could indicate a security incident.
- Bidder shall perform continuous vulnerability scanning and penetration testing of APIs to uncover and mitigate security weaknesses promptly.

2. **Cloud Service Security**

- Bidder shall ensure the activities and tasks associated with Cloud Service Security outlined as below
  - Cloud Computing Services (Public Cloud, Community Cloud, and Hybrid Cloud) are essentially "Outsourcing of IT Services". Accordingly, directions of the government and regulators on Outsourcing of IT Services or Cloud Security must be followed in letter and spirit.

- Governance Guidelines
  - Bidder shall ensure that the CSP undergoes periodic third-party security assessments and submits the related reports to the CSE to provide an objective evaluation of the CSP's security posture and gain assurance on the CSPs compliance with the prescribed policies, procedures, standards, laws, and regulations etc.
  - Bidder shall conduct regular training and awareness programs for its personnel to stay updated on the latest threats, technologies, and best practices related to Cloud Services.

- Technical Guidelines
  - Bidder shall ensure that the Cloud security measures must be developed, documented, and maintained
  - Bidder shall ensure that the CSP has a vulnerability management process in place to mitigate vulnerabilities in all components of the services that the CSP is responsible for. The Bidder shall also ensure that the CSP conducts Vulnerability Assessment and Penetration Testing (VAPT) for the components managed by the CSP and fixes the issues/ vulnerabilities within the prescribed timelines.
  - To ensure controls on encryption and Key management, the "Bring Your Own Key" (BYOK) approach should be adopted, where applicable, which will ensure that the MSLDC retains the control and management of cryptographic keys that would be uploaded to the cloud to perform data encryption. Wherever CSP is doing Key management for platform-level encryption (full disk encryption or VM level encryption), bidder should assess that CSP is doing the entire Key lifecycle management securely.
  - Bidder shall ensure that the CSP has controls in place to mitigate shared technology issues by at least deploying logical isolation and virtualisation techniques, implementing security best practices for installation and configuration, implementing strong authentication and access control for administrative access and operations, monitoring the environment for unauthorised changes and activities, conducting periodic vulnerability scanning and configuration audits, enforcing SLAs for patching and vulnerability remediation,
  - Bidder shall ensure that incident response, disaster recovery and business continuity procedures of the CSP meet the contingency planning requirements of the MSLDC.
  - Bidder shall put in place processes for continuously monitoring the security state of the on-cloud hosted information systems to support ongoing risk management decisions.
  - Bidder shall ensure that all logs of assets related to its subscription/ tenant are integrated with its SIEM/SOC for incident reporting and handling of incidents relating to services deployed on the cloud.
  - Bidder shall conduct regular training and awareness programs for its personnel to stay updated on the latest threats, technologies, and best practices related to Cloud Services.

3. In addition to the above bidder shall follow the applicable standards / practices of National Cyber-Security Reference Framework (NCRF) to improve the Cyber Security Posture.