Annexure-3 to Part-B

ONGC TRIPURA POWER COMPANY LIMITED

TECHNICAL SPECIFICATION

FOR

IMPLEMENTATION OF E-PROCUREMENT SYSTEM AT

OTPC

2 X 363.3 MW

GAS BASED COMBINED CYCLE POWER PLANT,

PALATANA, UDAIPUR, TRIPURA

TECHNICAL SPECIFICATIONS FOR IMPLEMENTATION OF E-PROCUREMENT SYSTEM AT OTPC

TABLE OF CONTENT

TECHNICAL SPECIFICATION OF IMPLEMENTATION OF e-PROCUREMENT SERVICES

1.0 It is clearly understood by the parties that in respect of Services to be provided by Contractor under the Contract, responsibility of Owner shall be limited to provide inputs related to procurement system followed at OTPC and Contractor shall be responsible for providing all other Services required for implementation and maintenance of e-procurement system for OTPC.

In this Technical Specification, capitalized terms used but not defined shall have the meaning assigned to them under the contract dated [●] (the "**Contract**").

2.0 GENERAL OBLIGATION OF THE CONTRACTOR

2.1 The Contractor shall obtain, at its expense, all Permits required to be obtained by the Contractor, to allow it to carry on its business and provide the Services under the Contract.

3.0 SCOPE OF SERVICES

3.1 In furtherance of and without limiting the obligations and responsibilities of the Contractor specified in the Contract, the Contractor shall, at all times commencing from the Effective Date and continuing through the Term and in accordance with the provisions of the Contract, perform the services specified hereunder (the "**Services**"). Any Services envisaged under the Contract to be provided by Contractor shall be provided as and when required.

3.2 The Contractor shall provide all the services required for successful and uninterrupted implementation, operation, maintenance, repair, update and upgrade of the **E-Procurement System** (**"EPS"**) in conformity with this Contract and Applicable Laws

3.3 Contractor shall implement web based comprehensive dedicated end-to-end e-procurement system for Owner for buying goods and services through quotations (RFP / RFQ), and tenders / bids {limited, open (eg. domestic, global)}.

3.4 Contractor shall implement e-procurement process for OTPC and shall work closely with working team members of OTPC for preparation of guidelines for bidder(s), hosting, managing and smooth execution of e-Tender/s. Any type of newspaper and other notification shall be the responsibility of OTPC. As part of this contract the following will be performed by the Contractor.

3.5 Contractor shall provide internet-based EPS on the following basis:

3.5.1 The EPS shall be provided on an Application Service Provider (APS) basis.

3.5.2 The EPS shall contain as minimum all features and functionality related to e-procurement specified herewith.

3.5.3 Contractor shall customize and configure its EPS as per the requirements of OTPC provided always that they shall be consistent with the scope of work.

3.5.4 Contractor shall provide integration of its EPS with third party service providers such as Digital Certification Providers, etc. approved by OTPC.

3.5.5 Contractor shall ensure hosting server capacity, related software, and internet connectivity in association with an appropriate Internet Service Provider for the hosting.

3.5.6 Data Retention: Transaction and master data of Owner shall be retained for 3 months after expiry of term of the Contract. Data shall be handed over to Owner in readable format after every 6 months of operations and expiry of the term of the Contract.

3.5.7 Data Backup: Database including transaction and master data shall be backed up and kept in secure storage every week.

3.5.8 Data generated by e-procurement system shall reside in Data Centers in India.

3.5.9 E-procurement system supplied shall be inclusive of hardware and software including but not limited to Operating System, Database, 3rd party software licenses, Data Center infrastructure, Disaster Recovery infrastructure, other hardware and software infrastructure.

3.5.10 Contractor shall operate and maintain the complete hardware and software system for the EPS on a 24 x 7 'round the clock' basis subject to scheduled maintenance downtime.

3.5.11 Contractor shall provide such system data and reports as may reasonably be required by OTPC.

3.5.12 Subject to adequate notice, contractor shall add or modify features and rules of the EPS as reasonably required by OTPC from time to time provided always that they shall be consistent with the scope of work.

3.5.13 Contractor shall provide in-person physical training for OTPC users and their bidders / contractors at Delhi and Palatana.

3.5.14 Contractor shall provide telephone, remote, and when necessary on-site troubleshooting support.

3.5.15 The Contractor will implement and maintain the EPS in such manner so as to minimize operating cost and maximize the system availability.

3.6 **Functional Specifications of proposed e-procurement system**: The application is intended to invite and accept online tender / quotations for OTPC. Major functions to be performed by the system are:

3.6.1 **Organizational Hierarchy**

3.6.1.1 Procurement Hierarchy: Users can be setup with association of roles, financial procurement powers, and other predefined parameters. Option to override default roles by higher-up authorities in hierarchy.

3.6.1.2 Jurisdiction definition: Jurisdictions with respect to area, financial limit for each department user can be predefined.

3.6.1.3 Roles Delegation: System should have facility of role delegation in case officials are going on leave or temporary outstation leave.

3.6.1.4 Tender opening committees for open, limited tenders etc.

3.6.2 **Vendor Registration & Management**

3.6.2.1 All existing vendors of OTPC shall be uploaded and shall create the individual vendor logins through mass upload route.

3.6.2.2 All vendors, who are not part of the OTPC vendor master shall be enrolled through the self-registration process.

3.6.2.3 Vendor debarment: System shall have a feature to debar a particular vendor for a particular time frame capturing the reasons for the same. During this debarment phase, the vendor will not be able to participate in any tender from OTPC.

3.6.2.4 Creation and update of dynamic centralized (master) or distributed (departmental) vendor database.

3.6.2.5 Attachment of supporting documents required for registration.

3.6.2.6 In-built document library for vendors to store credential documents, certificates, etc. for making it easy and quick to attach documents during tender submissions.

3.6.2.7 PAN number and GST number shall be the unique identifier key for vendors.

3.6.3 **Tender Management**

3.6.3.1 Tender Preparation: This section provides information on tender creation. User having tender preparation privilege will be able to create new tenders in the system. During the creation of enquiry, the system should be capable of handling unlimited line items and hierarchical level in one tender document.

3.6.3.2 Tender Authorization and Publishing: Tender authorization is the process of finalization of the tender created in the system. Authorizer is required to have a Digital Certificate for finalization and publishing of tender. Once a tender is authorized, it is available for the interested bidders to download and respond.

3.6.3.3 Publishing of Corrigendum's Amendments and Cancellation: Allowing the authorized user to Upload Corrigendum, Amendments, Pre-bid Clarifications and revise timelines and cancel the tender.

3.6.3.4 Sale and issuance of Tender Documents and Downloads: All registered bidders / suppliers will be allowed to participate in the tenders issued over the system.

3.6.3.5 Bid Preparation and Submission: In this stage the interested bidders prepare their bids online and store in secured format. The data is encrypted using the bidders Digital Certificate and hence lies in the bidders control.

3.6.3.6 In the bid submission stage, the bidders transfer the control of bid data to OTPC concerned department in a secured manner so that at the time of tender opening the data can be opened by authorized officers of OTPC.

3.6.3.7 Tender Closing, Opening and Evaluation: In the tender closing stage the authorized officer closes the tender which is equivalent to closing of tender box and generates super hash values. These values are made public to all bidders / applicants. Now no new bidders will be able to participate in the tender or will be able to edit their bids. No extension of Bid Preparation deadlines is possible. The application allows online secured opening and evaluation of the bid responses submitted by the bidder. The evaluator can provide comments and results of evaluation against individual evaluation criteria.

3.6.3.8 Selection of type of procurement with stages.

3.6.3.9 Creation of tender notifications with easy data duplication facility and attachments support provided for documents, image, specifications, drawings, and other scheduled attachments.

3.6.3.10 Bidding forms in various formats like excel, PDF, HTML etc.

3.6.3.11 Customizable templates for tender creation, bidding sheets, registration pages.

3.6.3.12 Support for open tenders to be called in single stage / two stage / three stage process.

3.6.3.13 Facility to host limited tenders with pre-qualified vendors.

3.6.3.14 Management of post tendering activities, such as auto generation of comparative statement.

3.6.3.15 Bid clarification module to seek additional documents from participating vendors during the technical and financial evaluation stage.

3.6.4 **Dashboard**: System shall have a customized dashboard which summarizes the overall e-procurement activities at a single glance for the users. Some of the predefine dashboard items are number of draft tenders, tender opening today, number of activated user, number of vendors due for EMD refund, number of tenders awarded etc., so all the useful information is only a single click away. This functionality shall be customizable as per OTPC requirement.

3.6.5 Technical Marking System or QCBS (Quality and Cost Based Selection) Evaluation Module is required.

3.6.6 **Accounting System**

3.6.6.1 Integration to prominent payment gateways for facilitating payments on real time basis and highly scalable and reliable payment platform.

3.6.6.2 Complete tracking of registration fee, tender form fee, EMD, security deposit, etc.

3.6.6.3 Capture of vendor's multiple bank account details during vendor registration process

3.6.7 **MIS and Reports**: The system allows generation of audit, evaluation and MIS reports.

3.7 **System Compliance Required:**

3.7.1 Standardization Testing and Quality Certification (STQC) guidelines on e-procurement;

3.7.2 OTPC's procurement guidelines;

3.7.3 Compliance to Information Technology Act 2000, govt. of India and all amendments thereafter;

3.7.4 Reserve Bank of India e-payment guidelines; and

3.7.5 Central Vigilance Commission (CVC) guidelines.

3.8 **Security Features Required:**

3.8.1 **Data Security**

3.8.1.1 User Access:

3.8.1.2 Access to system shall be through User ID & Password. Password change shall be as per OTPC's IT Manual provisions.

3.8.1.2.1 Roles defined by Admin shall be applicable to individual users.

3.8.1.2.2 Access control role delegations.

3.8.1.3 EPS shall be enabled to use digital signatures. Shall support digital signatures for documents, log-in and tender opening.

3.8.1.4 System should have PKI (Public Key Infrastructure) enablement for highest level of security.

3.8.1.5 Digital signature support for sensitive activities, such as uploading of documents, tender submissions and tender openings.

3.8.1.6 Tender document to be uploaded by the vendor should be signed by using Digital signature certificate.

3.8.1.7 EPS shall have option to verify any document against its digital signature.

3.8.1.8 Authorized department users with access rights only have the right to access bid information and open tenders on or after the stipulated date and time of tender opening.

3.8.1.9 When the vendor makes bid submission, the system will automatically generate a time stamp that will acknowledge the submission of the bid.

3.8.1.10 System shall have audit trail feature to display all the activities made in the system. Audit trail report for each tender to be made available as and when required.

3.8.1.11 The entire life cycle of the electronic tender is made available in MIS reports for recording the activities of buyer-side users and vendor activity (vendor registration, tender request, tender submission, awarding, etc.)

3.8.2 **Database and Document Security**

3.8.2.1 Vendor shall log-in using their PKI digital key and fill-up and upload their bid document to the site for submission to ensure legality of the bid submission.

3.8.2.2 Integration to virus detection tools to provide in-built online scanning for virus detection of all files before uploading is done by the vendor.

3.8.2.3 Confidentiality of the bids maintained by use of SSL 128 bit or higher encryption technology.

3.8.2.4 Vendor documents encrypted using both symmetric and asymmetric algorithms.

3.8.2.5 Documents saved in restricted domains accessible to only authorized personnel.

3.8.3 **Application Security**

3.8.3.1 EPS shall have application level access controls for viewing and updating of documents.

3.8.3.2 Access triggers for features activated based on user activities and tender date / time.

3.8.3.3 Do's and Don'ts within the application to ensure proper workflow.

3.8.3.4 Limited view based on access and limited access for activities.

3.8.4 **System Security**

3.8.4.1 SSL shall be implemented for secure data transmission.

3.8.4.2 System shall be secured through firewalls and antivirus systems.

3.8.4.3 Net manager and intrusion detector for online security.

3.8.4.4 Server time matching with Indian Standard Time (IST).

3.9 **Training & Support**

3.9.1 **Help Desk**

3.9.1.1 Well established help desk available for both contractors / vendors and buyer.

3.9.1.2 Increased visibility of tender through email alerts, SMS alerts, publication as free view in tender portals and scroll messages in home page.

3.9.1.3 Vendor query management system.

3.9.2 **Training**

3.9.2.1 Unlimited training to officials & bidders as and when required.

3.9.2.2 Mock training shall be imparted on all tendering activities.

3.9.2.3 Training on usage of digital signatures provided to each vendor.

3.9.2.4 Multi-lingual training support provided for new vendors.

3.9.2.5 Up to date user manuals on e-procurement activities.

3.9.2.6 Online e-learning help resources like view demo system.

3.9.2.7 Special training sessions to update users about new enhancements.

3.9.3 **Support Services**

3.9.3.1 24x7 e-procurement portal availability.

3.9.3.2 Technical support to address application issues.

3.9.3.3 Assistance provided to procurement officials by on-site / off-site deployment team.

3.9.3.4 Comprehensive training and support visits undertaken on request

3.9.3.5 Email notification for new tenders sent to registered contractors / vendors along with tender submission acknowledgement, payment transaction, confirmation, issue of new password, corrigendum, etc.

3.9.3.6 SMS sent to new tenders, corrigendum, submission and tender opening reminders.

3.10 The Contractor expressly agrees that the scope of work shall also include all such services which may not have been specifically mentioned in this Contract or the Scope of Work but which may be necessary required for the successful fulfilment of Contractor's obligation under this Contract as per Good Software Design and Engineering Practices and such services shall be performed by the Contractor without any additional cost to the Owner.

3.11 **Web Development Standards Required:**

3.11.1 System should be developed with the latest technology and established development tools and software utilizing modern web design and standards.

3.11.2 The development approach should conform to the best practices in the web development and maintenance industry.

3.11.3 Facility to update content by multiple users through browser based administrative module using a WYSIWIG editor.

3.11.4 System should be browser agonistic.

3.12 Application software shall be secured from network and cyber-attack**.**

3.13 A proper hashing algorithm encryption technique must be used for storing the sensitive information such as credentials in database.

3.14 It is ensured that SSL certificate is added in application software to prevent from browser based threats.

3.15 Security controls for the application software would be in conformity with latest legal and regulatory standards, Government of India guidelines, CERT-IN guidelines, IT Act 2000 as amended by authority from time to time.

3.16 The application software should have proper input validation to prevent XSS, SQL injection, buffer overflows and other input attacks.

3.17 The application software should have auditing and logging features enabled to audit and log access across application tiers, log key events, security of log files etc.