Intelligent Communication Systems India Ltd. (ICSIL)
(Joint Venture of TCIL – A Govt. of India Enterprise & DSIIDC – An Undertaking of Delhi Govt.)
Administrative Building, 1st Floor, Above Post Office, OkhlaIndl. Estate, Ph.-III, New Delhi -110020
e-mail: *info@icsil.in*, *www.icsil.in*

TENDER NO: F.1 (ICSIL)/03/220/GM(IT)/DTT FMS/2013-14/ Dated: 29.08.2013

SECTION -I

TERMS & CONDITIONS OF THE TENDER

1. Sealed quotations in two bid system are invited from eligible and competent firms having experience and expertise in providing Facility Management Services to a large IT government setup. Services of System Administrator, Network Administrator, Database Administrator, Security Administrator and Assistant Programmers having more than three years' experience in the relevant field are required initially for a period of one year to manage a large IT set up of a government department. The services of following personnel are required:

S.No	Manpower required	Nos.
1	System Administrator	One
2	Network Administrator	One
3.	Database Administrator	One
4	Security Administrator	One
5	Asstt. Programmer	Three

2. Detailed Tender Document containing eligibility criteria and other conditions are given here under. Last date for receipt of tender in ICSIL is 23.09.2013by 2:30 PM.

3. Tender time lines are as under:

Sl. No	**Description of activities**	**Tender Time-ines**
1	Last date for submission of Sealed Quotations	23.09.2013by 2:30 PM
2	Date and Time of opening of Technical Bid	23.09.2013by 3:00 PM
3	Date and Time of opening of Commercial Bid	Will be intimated on 23.09.2013

4. Eligibility Criteria:

1. The bidder should be an IT company of Indian origin and registered under Companies Act 1956 for the last **three**years.
2. Having more than **3 y**ears' experience in the IT field.

3. Average turnover of the bidder for the last three year i.e. 2010-11,2011-12 and 2012-13 should be minimum **Rs.25 Lakhs.**Bidder should submit certified copy of the same from the Chartered Accountant.

4. Must have back-end technical support in Delhi or NCR.

5. The bidder should have valid CST/VAT number as well as PAN number in the name of the firm. Proof should be submitted; failing which bidder's bid would become invalid & shall be rejected.

6. Attested copies of Articles of Association (in case of registered firm), By-laws & certificates of registration (in case of registered co-operative societies), partnership deed (in case of partnership firm) should be submitted.

7. The bidder should be registered with Service tax department of the Government of India. Enclose copy of the valid Registration Number.

8. A self-certificate that the bidder has not been black listed by any institution of the Central/State government in the past three years, is to be submitted.

9. The bidder should have expertise and experienced manpower in the relevant field to handle specific work. The particulars and educational qualification of the manpower to be deployed by the bidder for the said work should be given in the Annexure-IV.

10. The Bidders are requested to furnish documents to establish their eligibility (indicating the page number in the bid) for each of the above clauses as per compliance sheet i.e. Annexure-III. Relevant portions, in the documents submitted in pursuance of eligibility criterion mentioned above, should be highlighted. If tender is not accompanied by all the above documents mentioned, the same would be rejected.

11. **ICSIL reserves the right to seek fresh set of documents or seek clarifications on the already / submitted documents. All documents should be submitted in hardcopy.**

12. Upon verification, evaluation / assessment, if any information furnished by the Bidder is found to be false / incorrect or incomplete, their bid shall be summarily rejected and no correspondence on the same shall be entertained.

13. Brief description and value of similar assignments carried out in the last three years and the contact person in the client organizations along with their contact particulars.

14. Deviations to Tender conditions will not be accepted.

15. The bidder should submit a compliance sheet in a tabular form with respect to the eligibility criteria as given at Annexure-III.

16. All pages should be numbered, stamped and signed by the bidder.

17. Different weightage of marks have been allotted to the firms satisfying conditions like:

i) Having practical exposure to VAT departments Business Rules, Procedures, Acts & Rules etc. submit copy of the work order, if any, executed by the bidder in a VAT Department.
ii) Developed Application Software for VAT Department. submit copy of the work order, if any, executed by the bidder in a VAT Department.

18. Selection of the firm shall be made on the basis of Quality and Cost Basis selection (QCBS) as mentioned below:

a) Technical Evaluation and Weightage: Technical bid shall carry a weightage of 100 Marks(Part-A & Part-B) as per weightage given in Annexure-V. To qualify in the technical bid evaluation, a bidder has to obtain minimum 75 marks in Part-A & Part-B taken together to become eligible for opening of its Financial Bid. Financial Bid of the bidder securing less than 75 marks in the technical bid shall not be opened.

b) Financial bid of the technically qualified bidders will only be opened for evaluation. Financial Bid of the bidder which is comparatively lowest will be selected for award of contract.

c) In case the rates of two bidders are found lowest, the work will be awarded to the firm who has secured more marks in the technical evaluation.

5. Submission Of Bids/Tender Documents:

The sealed tenders should be submitted on or before the last date and time as given in the Tender timelines with superscription.

"TENDER NO:F.1(ICSIL)/03/220/GM(IT)/DTT FMS/2013-14/Dated: 29.08.2013" and submitted to:

General Manager (IT)
INTELLIGENT COMMUNICATION SYSTEMS INDIA IMITED
ADMINISTRATIVE Building, 1ST FLOOR,
ABOVE POST OFFICE, OKHLA INDUSTRIAL AREA, PHASE-III,
NEW DELHI-110 020.

A. Cover-1: Technical Bid:

i) Documents as required in the Tender shall be submitted in this envelope. The envelope should be sealed and superscripted "Technical Bid for Hiring IT Manpower". **Financial Bidshould not be** submitted in the envelopecontaining Technical Bid, failing which the bid will be rejected.

B. Cover-2: Financial Bid:

i. The envelope shall be sealed and superscripted "Financial Bid for Hiring IT Manpower". The financial bids of technically qualified bidders only shall be opened.

The above two envelopes shall be placed in one outer cover superscripted "ICSIL Tender**: F.1 (ICSIL)/03/220/GM(IT)/DTT FMS/2013-14/ Dated: 29.08.2013".**

ii. The outer cover shall be **submitted to the office of General Manager (IT), ICSIL on or before 23.09.2013by 2:30 PM i.e. by the last date and time for submission of the bid.**

iii. **Tender Processing Fee:** The bidders should submit a non-refundable Tender Processing Fee of Rs.2000/- (Rupees Two Thousand Only) in the form of Demand Draft Payable to ICSIL, Delhi.

iv. **EMD:** All bidders must submitted **an unconditional and irrevocable EMD for Rs.2,00,000/- (Rupees Two Lakh Only)** in the form of Bank Guarantee issued by a nationalized commercial bank valid for a period of 180 days from the date of issue in favor of Intelligent Communication Systems India Limited, Delhi.

v. The tender Processing Fee & EMD should be submitted along with Technical Bid in separate cover super scribed as "EMD & Tender Processing Fee". **Tender** without Tender Processing Fee and EMD shall be rejected.

vi. Bidders registered with SSI or NSIC and having proof of exemption **for similar work or** items only are exempted from submission of Tender Document and EMD Fee provided they submit valid documentary proof for the same in their name.

vii. Financial Bid of only those bidders who are found qualified in technical bid will be opened for evaluation.

viii. The work order shall be awarded to lowest quoted firm derived by summing up the cost of all items. Final decision in this regard shall vest with ICSIL. **In exceptional circumstances, ICSIL reserves the right to award the contract to L2 bidder on technical grounds with full justification.**

ix. Successful bidder awarded with the work order shall have to submit Performance Bank Guarantee or Bank Draft or Pay Order valid for a period of one years or extended period for an amount equal to 10% (Ten Percent) of the total project cost in favor of intelligent communication Systems India Ltd, Delhi.

x. No interest shall be payable to the bidders either on EMD or Performance Security.

6. Release of EMD:

i) EMD of unsuccessful bidders will be released immediately once the work order is placed on the successful bidder.

ii) EMD of Successful bidders shall be returned after the work order is awarded and Performance Guarantee in the form of Bank Guarantee valid

for a period of one years or Bank Draft or Pay Order for requisite amount in favour of Intelligent Communication Systems India Ltd, Delhi is submitted.

7. Payment Terms:

i) No advance payment shall be made.

ii) Payment to the firm shall be made on back to back basis after submission of bills. A certificate to this effect certifying satisfactory services shall be submitted from the concerned department.

iii) Bill for release of payment should be submitted in triplicate along with satisfactory completion certificate from the client department for the activity/Task for which the bill is being raised. In the absence of satisfactory completion certificate from the client department, the bill for payment shall not be processed and released.

8. Penalties:

A. For unauthorized absence:

In case of unauthorized absence beyondthree consecutive days, a penalty of Rs.1500/-perabsentday from first day of absence up to a maximum of seven days will be imposed.

B. For Not providing substitute:

In case any personnel proceeds on leave for more than seven days and his substitute is not provided for the leave period, a penalty @Rs.2000/- per day from 8th days of absent and up to a maximum period of 15 days shall be imposed. In case the substitute is not provided even after 15 days, the contract for that particular service will be terminated and a penalty of Rs. five lakh shall also be deducted from the dues or performance guarantee of the bidderfirm**. It is clarified here that for default of clause 8(A) and 8(B) both, the penalties will run simultanelusly.**

9. Validity Of Tender:

The Tender is valid for a period of six months (i.e. 180 days) from the date of publication of the tender. The validity time may be extended by ICSIL.

10. Validity of Rates:

i) The rates shall be valid for a period of one year and the contract extended period from the date of issue of work order. Vendor shall be bound to provide the services on the same rate and terms and condition for the extended period.

ii) MD ICSIL reserves the right to cancel/ terminate the tender at any stage in whole or in parts without assigning any reason.

11. Commercial bid:

i) Bidders should quote prices as per commercial bid format given at Annexure-II

ii) Rates should be inclusive of all taxes, duties and levies.

12. Forfeiture of EMD:

EMD can be Forfeited under the following circumstances :

i. If the bidder withdraws its bid after last date of submission of bid,
ii. Fails to execute the work order within given time.
iii. Fails to submit requisite Performance Guarantee with in prescribed period.
iv. Furnishes wrong information,

13. Forfeiture of Performance Guarantee:
Performance Guarantee can be Forfeited under the following circumstances:

i. Fails to deploy manpower as per given timeline
ii. Services of manpower not found satisfactory.
iii. Suitable substitute is not provided after 15 days of absent of any employee.

14. Other Conditions:

i) Rates should be quoted as per the format of commercial bid.
ii) Rates should not be quoted in the Technical Bid.
iii) Payment shall be made on actual basis on back to back basis.
iv) If any bid is found non-complying with above criteria including Terms & Conditions of the Tender etc., that bid shall be summarily rejected.
v) Firm awarded with the work order shall deploy its resources within 10 days of the receipt of the work order
vi) Firm shall deposit Performance Guarantee of the requisite amount within 10 days of the receipt of the work order.

SECTION-II

SCOPE OF WORK

A. Existing Platform:

The Department is currently having the following platform for which services of suitable on-site System Administrator, Network Administrator, Security Administrator, Database Administrator and Asstt. Programmers are being hired. The Servers are installed at NICSI Data Centre as well as in the department. Following are the details of the existing platform in the department:

Product
Windows Server 2008 R2
Database – MS SQL SERVER 2012
Microsoft .Net 4.0
Dynamics CRM 2011
Microsoft Share Point Portal Server 2010

iii) Network:

S.No	Product Description	Total Qty.
1.	Core Switch as per technical specifications	2
2.	Access Switch	64
3.	Router	2
4.	Internet Firewall with IPS	2
5.	Event logging, monitoring and reporting	1
6.	Network Access Control	1
7.	Network Manager	1

B. Duties and Responsibilities of the individual incumbent:

1. **System Administrator (SA):**

IT Systems Administrator will be responsible for the configuration, implementation, and maintenance of various technologies available in the department. This person will focus on the administration of application software and infrastructure to include desktop PC's, serversand software applications. SA Shall work under the direction of IT head of the department. This position requires excellent customer service and organizational skills to support departmental personnel and clients. This position requires the ability to function successfully in both team and independent work environment.

DUTIES AND RESPONSIBILITIES:

- **i.** Assist in the planning, design, documentation, and implementation of various systems to include desktop PC's, servers, and software applications.
- **ii.** Develops, maintains, and monitors procedures for all server backups.
- **iii.** Monitors, plans, and coordinates the distribution of client/server software and service packs.
- **iv.** Perform on-site and remote technical support.
- **v.** Assist in the organization and inventory of all hardware and software resources.
- **vi.** Maintains excellent communication with the IT Head on all tasks and projects.
- **vii.** Create and maintains good technical documentation.
- **viii.** Provide network and desktop support to over 1200 users and other stakeholders
- **ix.** Install and test computers, Servers and related network hardware in a LAN/WAN environment.
- **x.** Oversee server configuration maintenance and management
- **xi.** Ensuring data is backed up on a regular basis using Backup software
- **xii.** Overseeing computer security and anti-virus updates etc.
- **xiii.** Carrying out client computer maintenance
- **xiv.** Providing IT support to computer users within the office
- **xv.** Troubleshooting of IT problems and resolving
- **xvi.** Liaising and communicating with external support companies/OEMs
- **xvii.** Overseeing file management on centralized resource (i.e. File Servers, Virtualization Server, Web Servers and Application Server) or on individual workstations
- **xviii.** Train IT staff on the computer systems as and when required
- **xix.** Keeping inventory of hardware and maintenance records
- **xx.** Ensuring that all software is properly licensed and up to date
- **xxi.** Keep abreast of IT technology, maintain library of information
- **xxii.** Advising on training needs and courses available
- **xxiii.** System Administrators (SAs) shall be technicians who administer, maintain, and operate information systems. They are responsible for implementing technical security controls on computer systems and for being familiar with security technology that relates to their system.

- **xxiv.** The System Administrator shall:
    a. Add, remove, maintain system users and configuring their access controls to provide the users necessary access with least privilege.
    b. Provide lists of system users for systems under his/her control and providing the lists to the appropriate users' managers and appropriate Security Administrator for review, update and certification;
    c. Configure system parameters within the documented security standards, using system life cycle documentation;

d. Maintain current documentation, if any, that properly defines the technical hardware and software configuration of system and network connections for systems they are responsible;
e. Ensure the proper installation, testing, protection, and use of system and application software;
f. Install and manage application server software including development tools and libraries, software compilers, code builds, and middleware interfaces between servers and application servers and back-end storage media,
g. Install and manage servers and workstation software for the OS in use.
h. Start up and shut down the system;
i. Perform regular backups and recovery tests and other associated contingency planning responsibilities for systems for which they are responsible;
j. Enable, configure, and archive audit logs/trails and system logs for review by the System Administrator for all systems,
k. Monitor system/user access for performance and security concerns;
l. Establish conditions on the system so that other operational entities can perform application management activities; and
m. Run various utilities and tools in support of the Security Administrator.

xxv. The SA shall be responsible for supporting the Security Administrator's needs for read access to system resources,

xxvi. Depending on the environment, the SA may perform user support for password issues. This can include (but is not limited to) resetting or issuing a new password when the user forgets the current one or locks the account.

xxvii. The SA shall install security patches in a timely and expeditious manner

xxviii. Support IT Contingency Plan and DR Plan development and accuracy.

Educational & Technical Qualification:
Minimum Bachelor's degree or higher qualification with MCSE or any equivalent Microsoft certification

Skills and Abilities and Experience:

Minimum three years' experience with Windows Server 2008 R2 platforms with an emphasis on Active Directory. A strong background of Dynamics CRM 2011, and Microsoft Share Point Portal Server 2010 is a must. Basic Windows scripting skills are also required.

2. Network Administrator:

1. Network Administrators (NAs) shall be responsible for the day-to-day administration of the network device.
2. At a minimum, the NA shall:

a. Configure network device parameters within the documented security standards, using the applicable policies and system life cycle documentation;

b. Ensure the proper installation, testing, protection and use of network device software, including installing network software fixes and upgrades;
c. Maintain the configuration of wireless networks or network devices under his/her control in accordance with the requirements of laid down standards,
d. Enable and configure audit logging on all systems in accordance with Audit Logging Security Standards and all other applicable configuration standards;
e. Maintain current documentation that properly defines the hardware and software configuration of the network devices and connections for which they are responsible;
f. Ensure inventories are accurately maintained;
g. Recommend and implementing processes, changes and improvements to programs, procedures and network devices;
h. Monitor network performance; performing network diagnostics; analyzing network traffic patterns; and
i. Support disaster/recovery planning, documentation, and implementation efforts for the network.

3. The NA shall support CERT-IN efforts and security incident handling.
4. The NA shall apply patches and hot fixes as directed, following configuration management policies and procedures.
5. The Network Administrator will be responsible for the configuration, implementation, and maintenance of various technologies managed by the Information Technology department. This person will focus on the administration of Departments' network infrastructure to include desktop PC's, servers, network equipment. Works under the direction of the Head of Information Technology Department.This position requires excellent customer service and organizational skills to support administrative personnel, department supervisors, staff, and clients.
6. Promote a positive work environment by maintaining respectful interactions with Staff members. This position requires the ability to function successfully in both team and independent work environments.

DUTIES AND RESPONSIBILITIES:

i. Assists in the planning, design, documentation, and implementation of various systems to include desktop PC's, servers, network equipment and software.
ii. Perform on:

-site and remote technical support.

iii. Assist in the organization and inventory of all hardware and software resources.
iv. Maintains excellent communication with the IT Manager on all tasks and projects.
v. Creates and maintains good technical documentation.
vi. Provides emergency on

-call support on a rotating schedule.

vii. Performs other duties as assigned.

viii. Provide network and desktop support to over 1200 users in 13th floors of the building of the department.

ix. Provide Voice

-over IP support and management to 13 floor of the building.

x. Designs, installs, upgrades, configures, and repairs local and wide area network hardware and infrastructure.

xi. Support Video Conference for all offices in the Wide Area Network, if required.

xii. Installs and tests computers and related network hardware in a LAN/WAN environment.

xiii. Maintains network maps of all sites.

xiv. Train branch staff with simple network troubleshooting techniques.

xv. Oversee network configuration maintenance and management

xvi. Overseeing computer security and anti-virus updates etc.

xvii. Liaising and communicating with external support company (i.e. Juniper etc)

xviii. Keeping inventory of hardware and maintenance records

xix. Ensuring all software is properly licensed and up to date

Educational and Technical Qualification:

Minimum Bachelor's degree or higher qualification with MCSE / CCNA certification. Must have more than Three years of NetworkSupport experience for Juniper Network products.

Skills and Abilities:

a) Three or more years' experience with Windows Server 2008 R2 platforms Solid knowledge of LAN/WAN configurations to include experience with Juniper routers & switches, Internet firewalls, and wireless technology etc. Network Management and Event logging/ monitoring/reporting for better management and proactive monitoring.
b) Network Access Controller for LAN users.
c) Firewall/IPS in HA mode (High Availability) to ensure that Network is highly secure from outside attacks/threats.
d) Security is considered on high priority to ensure that Confidentiality, Integrity and Availability of Data is maintained.

3. Database Administrator:

Database Administrator role and responsibilities

The Database Administrator is responsible to resolve problems and ensures that the application is running well with respect to the database. He should be familiar with schema and objects, Management of tables and indexes.

The Database Administrator shall perform the following responsibilities:

A. Backup and recovery

i. Performs periodic backups
ii. Has full knowledge of the restore procedure
iii. Monitoring database activity

B. The Database Administrator must understand the following:

i. When transaction rollbacks occur
ii. When the database is out of system disk space
iii. When unique constraints have been violated (this can be accomplished by using alerts)
iv. When not to shutdown the database while the application is running

C. Performance

i. Take immediate action when performance issues arise:

a. Analyze SQL statements and if some are taking an inordinate amount of time to run, determines the cause:

i. Explain plan
ii. Checks updated statistics

ii. Monitor when the database performs a rollback on a very large transaction causing performance issues with other transactions
iii. Verifies that the database is running in an optimized fashion, not only at the system level but at the level of tables and queries as well
iv. Tunes procedure for gathering statistics to obtain optimal performance
v. Calculates how often statistics need to be updated to obtain optimal performance
vi. Reorganizes the tables and indexes at regular intervals of time

D. Locks

i) Analyzes where locks are coming from

a. Gets trace of SQLs
b. Matches SIDs to server or process

i. Detects deadlocks
ii. Checks why the source of the block is still blocking

a. If it is a long running job because of slow running SQLs

b. Why are the SQLs slow?
i) Perhaps the DB is doing a rollback on a session and the application is still generating SQLs
ii) Maybe it is a bad explain plan (check SQL performance)
iii. Possibly the DB is doing a rollback on a transaction
iv. Size of the transaction could be a factor

The Duties and Responsibilities:

i. Providing on-site support services for MS SQL, Dynamics CRM 2011, Microsoft Share Point Portal Server 2010

ii. Shall be responsible to undertake all changes including fine tuning, configuration and reconfiguration of MS SQL components as and when necessitated.

iii. Maintain proper documentation of all the configurations done, changes made etc.

iv. Evaluate overall performance of databases and Application Servers and take necessary measures to improve performance.

v. Resolve all critical support issues notified by the customer.

vi. Bug report, filing, tracking and reporting

vii. MS SQL and Application Server installation as and when required.

viii. The person deputed by the firm shall act as **database administrator** and shall be responsible for the following activities:

a. MS SQL Architecture & Tuning

i. Demonstrate an understanding of the memory structures & Processes that make an MS SQL Instance

ii. Demonstrate an understanding of Physical & Logical Structure associated with MS SQL Instance

iii. Demonstrate an understanding of PL/SQL constructs (triggers, functions, packages, procedures)

iv. Demonstrate an understanding of Distributed Architecture & Client Server

b. Security

i. Create, alter & drop database tables and users
ii. Monitor & audit database access
iii. Develop & implement a strategy for managing security (roles, Privileges, authentication)

c. Data Administration

i. Manage Integrity Constraints
ii. Implement the Physical Database from the Logical Design
iii. Evaluate the implications of using stored procedures & constraints to implement business rules

d. Backup & Recovery

i. Understand Backup Options

ii. Develop Backup & Recovery Strategies like cold backup, export backup and on-line RMAN backup.

iii. Manage the implementation of backup procedures

iv. Recover a Database

e. Software Maintenance & operation

i. Install & Upgrade MS SQL& other supporting software
ii. Configure the MS SQL instance using the initialization parameters
iii. conversant with Startup & Shutdown options
iv. Create Databases
v. an understanding of the capabilities of underlying Operating Systems as they relate to MS SQL

f. Resource Management

i. Create & Manage Indexes
ii. Evaluate the use of Clusters & Hash Clusters
iii. Allocate & Manage Physical storage structures (Data Files, Redo Logs, Control Files, archive logs, parameter file (pfile), and stored parameter files (spfile).
iv. Allocate & Manage Logical storage structures (Tablespaces, Schemas, Extents)
v. Control system resources usage by defining proper profiles
vi. Perform Capacity Planning

g. Application Server Administration

i. Performance tuning of Application Server Components etc
ii. Review, Maintenance and Back-up of Log/Trace files of various components of Application Server
iii. Installation and Configuration of Application Server
iv. Review of Application users, sessions, etc.

h. Tuning & Troubleshooting

i. Diagnose & resolve locking conflicts
ii. Use data dictionary tables & views
iii. Monitor the instance
iv. Collect and analyse relevant database performance information including System Performance Report (SP Report).
v. Identify & implement appropriate solutions for database Performance problems
vi. Use vendor support services, when necessary
vii. Solve all SQL related system tuning problems

I. Other Responsibilities:

i. Planning the database & making sure that the database Server has enough memory and disk storage to accommodate proposed system

ii. Installing necessary software on the server

iii. Creating MS SQL Database

iv. Managing space requirement for the database

v. Creating database objects, such as Tables & Views

vi. Creating New Users & Managing user privileges

vii. Backing up database on regular basis

viii. Recovering database whenever necessary

ix. Controlling access to the database using security features

x. Monitoring & tuning Database

xi. Configure & Tune SQL

xii. The Database Administrator (DBA) shall perform all activities related to maintaining a correctly performing and secure database environment. Responsibilities include design (in conjunction with application developers), implementation, and maintenance of the database system.

xiii. The primary security role of any Database Administrator (DBA) is to administer and maintain database repositories for proper use by authorized individuals.

xiv. DBAs shall have the least level of elevated privileges required to perform DBA-related duties and shall not have system administration capabilities.

xv. At a minimum, the DBA shall:

a. Establish security for database objects within the database and for the DBMS according to security policies;
b. Support disaster/recovery planning, documentation and implementation efforts for the database(s);
c. Establish database points of consistency;
d. Coordinate with the SA to integrate database backups into the system related backup and recovery, including creating the backups if necessary;
e. Periodically test backup copies of the databases;
f. Recover the database to a current or previous state, if necessary;
g. Recover individual objects (e.g., data rows, etc.) to a current or previous state;
h. Identify database requirements of system resources;
i. Provide network requirements for the database to the organizations responsible for designing and implementing network services;
j. Manage the database configuration (e.g., architecture, internal settings, etc.) according to the certified and accredited operating system security configuration;
k. Support Security Assessments and Authorization efforts;
l. Monitor/manage database performance and capacity;
m. Monitor user activities where appropriate; and

n. Enable and configure audit logging on all systems in accordance with Audit Logging Security standards.

Educational and Technical Qualification:

Minimum Bachelor's degree or higher qualification. Must be Certified Microsoft Database Administrator having more than five years working experience of Database Administrator on MS SQL Server and related tools.

4. **Security Administrator:**

The Security Administrator role is responsible for all security attributes of a user or role. The security administrator is responsible for the following tasks:

i. Approving new divisions (administrative levels) in the organization
ii. Approving new users in the organization
iii. Approving user service requests
iv. Denying password resets to those who cannot properly validate their identity
v. Editing the organization profile
vi. Editing user profile
vii. Filtering invalid requests

Security Administrator Responsibilities for Users:

i. Assigning and modifying the security attributes of a user, role, or rights profile
ii. Creating and modifying rights profiles
iii. Assigning rights profiles to a user or role
iv. Assigning privileges to a user, role, or rights profile
v. Assigning authorizations to a user, a role, or rights profile
vi. Removing privileges from a user, role, or rights profile
vii. Removing authorizations from a user, role, or rights profile

Typically, the Security Administrator role creates rights profiles. However, if a profile needs capabilities that the Security Administrator role cannot grant, then superuser or the System Administrator role can create the profile.

Before creating a rights profile, the security administrator needs to analyze whether any of the commands in the new profile need privilege or authorization to be successful.

Security Administrator

1. The Security Administrator shall be responsible for reviewing all activities of the SAs, NAs, DBAs, anyone responsible for the operation or administration of IT infrastructure.
2. The Security **Administrator** shall oversee any and all user (e.g., system, database, application, etc.) administration regardless of how or who performs it.

3. Additionally, **Security Administrator** shall:

A. Ensure the site contingency plans remain up-to-date in response to new security requirements;
B. Conduct and support all security reviews of systems and networks;
C. Provide or recommend security measures and countermeasures based on the security reviews and security policies;
D. Upon management request, review individual user's access verifying it is the least privilege necessary to perform his/her job;
E. Inspect and monitor user files, as directed by management;
F. Conduct security audits, verifications and acceptance checks, while maintaining documentation on the results;
G. Promote security awareness and compliance;
H. Report security incidents including those discovered while reviewing audit logs/trails; and
I. The **Security Administrator** shall review all types of audit logs/trails and observe system activity at least weekly in order to:

i. Ensure integrity, confidentiality and availability of information and resources;
ii. Detect inappropriate user and system actions that could be construed as security incidents;
iii. Investigate possible security incidents; and
iv. Monitor user or system activities where appropriate.

4. A **Security Administrator** shall not perform system/security administration on any system/platform/application, etc.
5. The **Security Administrator** shall have read-only access to system resources and shall not modify audit settings.
6. Follow any applicable organizational-level incident reporting procedures (such as contacting management, system administrators, or the Computer Emergency Resource Team India (CERT-IN) in the event that evidence of suspicious activity is discovered in the course of reviewing security audit log information.
7. **Security Administrator** shall be concerned with the security and integrity of the database and responsible for:
   A. Ensuring that DBAs, System Administrators (SAs), and others having daily operational responsibilities comply with the security requirements. In general, the **Security Administrator** is not expected to personally implement the requirements, but rather ensure that others do so; and

B. Report non-compliance issues initially to DBAs and SAs for resolution, and escalate non-compliance reporting to management as necessary to bring systems into compliance with security provisions.

C. Not have operating System Administrator privileges.

8. **Educational and Technical Qualification**:

Minimum Bachelor's degree or higher qualification with MCSE / CCNA certification. Must have more than Five years of Security Administrator or Network Administrator experience.

5. Asstt. Programmer:

Asstt. Programmer shall be responsible to conduct feasibility study of the department, understand the software requirement of the department and prepare documents for Functional Requirement Specifications, Software Requirement Specifications and Software Design Document (SDD). Based on SRS & SDD, undertake software development, Test the software on test data, imparting training to the end-users and thereafter roll out of the application.

Educational and Technical Qualification:

Minimum Bachelor's degree or higher qualification with minimum three years of working experience of software development on the following platforms:

i) Windows Server 2008 R2
ii) Database – MS SQL SERVER 2012
iii) Microsoft .Net 4.0
iv) Dynamics CRM 2011
v) Microsoft Share Point Portal Server 2010

4. LOCATION OF WORK

Firm awarded with the contract shall work in the Trade & Taxes Department, Vyapar Bhawan, I.P. Estate, New Delhi on 365 x 7 basis.

5. DELAY IN PERFORMANCE

The Service Provider shall be responsible to maintain 100% uptime for database and other components covered under the contract. In the event of major failure of the system, the service provider shall make all possible effort to bring the system up by following day before the start of office time.

6. EXCLUSIONS

Neither the firm nor the department shall be liable to each other for the delay in or failure of performance on their respective obligations under this contract caused by occurrences of events beyond the control of the parties known as force majeure including but not limited to fire (including failure of reductions) acts of God, act of Public enemy, war, insurrections, riots, strikes, lockouts, sabotage, any law statutes or ordinance, order, action or regulations of the Governments or any agencies thereof or any other local authority, or any compliance therewith or any other cause, contingencies or circumstances similar to the above. On the happening of the one or any more of the above event, either party shall promptly but not later than five days thereafter notify in writing to other of the commencement and cessation of such status/tenure of force majeure condition or the said contingency, and of such condition, contingency continues beyond one month then both the parties will discuss to find out a fair and equitable solution to solve the stalemate or for termination of this contract or otherwise decide the course of action so that both the party's interest may not suffer adversely.

7. TAXES

Department shall not pay any other taxes except those mentioned by the firm in the Commercial Bid. The liability to pay taxes not mentioned in the commercial bid shall vest with the service provider.

8. INDEMNITY

The firm awarded with the contract shall effectively indemnify and hold the department harmless from any loss, claim or damage including any claim as to death or personal injury to any person deployed by the firm in the department. The service provider shall be responsible for any loss arising out of any failure on the part of the employee deputed by the service provider to keep full and up to-date back-up of data and system files, programs.

9. CONFIDENTIALITY

The firm awarded with the contract shall maintain complete secrecy of all documents/data/software or any other related information. The firm shall not publish, disclose any information about, make available or otherwise dispose of the document/ data/ software or any part or parts thereof to any third party, directly or indirectly without prior written consent of the department.

****

Annexure-II

Commercial Bid Format

Note: Prices should be inclusive of all taxes, duties and levies, if any.

Rates should be quoted as per qualification and experience desired in the Tender.

S.No.	**Item Description**	**Nos.**	**Unit Rate**	**Total Amount**
1.	Assistant Programmer	3		
2.	System Administrator	1		
3.	Network Administrator	**1**		
4.	Security Administrator	**1**		
5.	Database Administrator	**1**		
	Total Amount:			
	Total Amount in Words:			

ANNEXURE III

TECHNICAL ELIGIBILITY COMPLIANCE SHEET

Note:. All pages should be stamped and signed by the bidder.

S.No	Eligibility Condition	Compliance to eligibility conditions (Yes/No)	Page NO.
1	The bidder should be an IT company of Indian Origin and registered under companies Act 1956 for the last three years.		
2.	The bidder should have more than three years' experience in the IT field		
3.	Must have back-end technical support in Delhi		
4.	Tender Document Fee for Rs,2000/-		
5.	EMD for Rs.2,00,000/- (Rupees Two Lakh)		
6.	The company should have valid CST/VAT number		
7.	The company should have valid PAN in the name of the firm.		
8.	Attested copies of Articles of Association (in case of registered firm), by laws & certificates of registration (in case of registered co-operative societies), partnership deed (in case of partnership firm) should be submitted.		
9.	The bidder should be registered with Service tax department of the Government of India.		
10.	A self-certificate that the bidder has not been black listed by any institution of the Central/State government in the past three years, is to be submitted.		
11.	Whether having practical exposure to VAT departments' Business Rules, Procedures, Acts & Rules etc. submit copy of the work order, if any, executed by the bidder in a VAT Department.		
12.	Brief description and value of similar assignments carried out in the last three years and the contact person in the client		

	organizations along with their contact particulars.		
13.	Turnover of the bidder during:		
	2010-11		
	2011-12		
	2012-13		

ANNEXURE-IV

Details of the personnel to be deployed on the Project

Category of personnel	**Name of candidates**	**Details of Qualification, Experience and certificationspertaining to** Windows Server 2008 R2, Database – MS SQL SERVER 2012 , Microsoft .Net 4.0, Dynamics CRM 2011, Microsoft Share Point Portal Server 2010		
		Qualification	**Experience**	**Certifications**
Database Administrator				
System Administrator				
Network Administrator				
Security Administrator				
(1) Asstt. Programmer				
(2) Asstt. Programmers				
(3) Asstt. Programmer				

ANNEXURE - V

TECHNICAL EVALUATION SHEET

Total Marks: Part (A) + (B)=100 Qualifying Marks: 75

Part-A. Technical Qualifying Criteria (Max. Marks:70)

S.No	Eligibility Criteria	Maximum Marks
1	The bidder should be an IT company of Indian Origin and registered under companies Act 1956 for the last three years.	**5**
2.	The bidder should have more than three years' experience in the IT field	**5**
3.	Must have back-end technical support in Delhi or NCR. submit proof	**5**
4.	Tender Document Fee for Rs,2000/-	**2**
5.	EMD for Rs.2,00,000/- (Rupees Two Lakh)	**2**
6.	The company should have valid CST/VAT number	**2**
7.	The company should have valid PAN in the name of the firm.	**2**
8.	Attested copies of Articles of Association (in case of registered firm), by laws & certificates of registration (in case of registered co-operative societies), partnership deed (in case of partnership firm) should be submitted.	**2**
9.	The bidder should be registered with Service tax department of the Government of India.	**2**
10.	A self-certificate that the bidder has not been black listed by any institution of the Central/State government in the past three years, is to be submitted.	**2**
11.	Whether having practical exposure to VAT departments' Business Rules, Procedures, Acts & Rules etc. submit copy of the work order, if any, executed by the bidder in a VAT Department.	**8**
12.	Brief description and value of similar assignments carried out in the last three years and the contact person in the client organizations along with their contact particulars.	**10**
13.	Turnover of the bidder during:	**8**
	2010-11	
	2011-12	
	2012-13	
	Total Marks	**55**

Part-B: Details of the personnel to be deployed on the Project (Max. Marks: 30)

Category of personnel	**Details of Qualification, Experience and certifications** Windows Server 2008 R2, Database – MS SQL SERVER 2012 , Microsoft .Net 4.0, Dynamics CRM 2011, Microsoft Share Point Portal Server 2010			**Max. Marks**	
	Qualification	**Experience**	**Certifications**		
Database Administrator				**9**	
System Administrator				**9**	
Network Administrator				**9**	
Security Administrator				**9**	
(1) Asstt. Programmer				**9**	
(2) Asstt. Programmers					
(3) Asstt. Programmer					
Total Marks					**45**
Total Marks (A) + (B)					**100**