1. Scope of Work:

1.1 Server OS Administration, Server Services Management and Storage management

1.1.1 Server OS Administration

Stand Alone servers and Virtual servers (VMware, Hyper-V) should be managed by Vendor and will include the following along-with all other actions, which are necessary for optimum utilization of the Servers and ensure availability, reliability and security of various services: -

a) Management and Configuration of Virtual environment, Vmware Vcentre Server, Hyper-V and Hosts.

b) Creation of New Standalone Servers and also Virtual Servers; including allocation of resources. Installation and configuration of Operating Systems OS, various applications and required services.

c) Weekly monitoring of Servers for the Network connections and troubleshooting, resolving server operational problems like system 'hang', hard disk crash, network connection failure etc. and keeping a log of the same. (8 hours). For this activity vendor has to send one expert engineer once in a week for complete day 8 Hours. ITER-India can demand the engineer of particular specialization.

d) Re-installation and support for Operating Systems running on Server e.g. Windows, LINUX and other System Software, as and when required.

e) Installation of packages, services, upgrades and patches of OS and other Software, as and when provided by ITER-India or OEM (Original Equipment Manufacturer

f) Downloading of various upgrades, bug fixes, updates, OS patches, Service packs, Security patches of OS and other System Software from OEM Web sites / provided by ITER-India Organization, as and when released, and installation of the same. These Patches shall be installed only after checking the same in the test environment, provided by ITER India. Keeping a log for the same.

g) Monitoring of resources like CPU utilization, memory utilization, disk space usage, swap utilization, average load, Systems network traffic etc. vis-à-vis thresholds using basic Server Management tools available on servers. Else Vendor may arrange tools for the same.

h) Provide Connectivity Management Services such as: -

- Creation of routes on servers to enable organization-wide access.
- TCP/IP Management.
- Network troubleshooting with tools like snoop, trace route, nslookup etc.
- Time synchronization between various servers using NTP Services.

i) Restoration of operation of Servers back after any failure using backup data.

j) Recovery of data in case of Hard Disk or System crash.

k) Performance management like kernel parameter optimization. Performing quarterly system performance tuning for optimum performance. Changing the system configuration parameters and re-organization the Disk space etc.

l) Escalating unresolved problems to OEM / Principal / Vendor for ensuring resolution.

m) Support for installation & smooth running of various Services running on these Servers.

n) Capacity planning on the Servers.

o) Ensuring confidentiality of the data.

p) Hardware Monitoring & other warnings, system alerts in Syslog like CPU panics & SCSI fatal error etc.

q) Provide support for Storage Management, such as: -

- Configuring disk arrays, RAID 5 etc.
- Disk and file System cleanups & maintenance using System commands.
- Automation of disk cleanup operations.
- Adding new file systems, logical volumes and correcting file system inconsistencies.

r) Provide support for Windows domain controller Management and Configuration of various services like DNS, FTP and & RAS and following activities for Window 2000 / 2003/2008/2012 Servers.

- File level and share level access control
- Security updates and OS Patch management
- Hot Fixes and service packs for OS
- Group and system policies implementation.
- Share & access point controls.
- Maintaining Active Directory services
- Configuration and maintenance of DFS (Distributed file system) and file replication services.
- Implementation for polices as per requirement

s) Performing periodic backup / restore of system files / volumes and maintain list of all systems, root directories and volumes and back up of the file systems.

t) Security management – Configuring Account policy, Access rights, Password control.

u) Verify logs in event logger and periodically clean up log files.

v) Ensure all critical services are running on the servers.

w) Take backup of the file systems and verifying the all system backups by periodically restoring the same.

x) Ensure that Networks, Servers are kept virus / worn free. Anti-Virus software will be provided by ITER-India. However, Vendor shall be required to arrange download of latest anti-virus updates from the Internet.

y) The Vendor shall be responsible for upkeep of server racks and server rooms, maintenance of records / registers, logs, standard operating procedures, procedure for shut down and restart of servers, backing-up and clearing of server logs.

z) Using the server management tools provided by ITER-India, following reports for Windows OS based will be generated within the overall capabilities of the tools.

Server related Reports	Frequency
Server Availability and Utilization Report	weekly
Server Capacity Planning Report	Weekly, Monthly
Server Configuration and Administration Manual – document containing processes for user creation / deletion / movement, folders, access, server monitoring and housekeeping, backup and restore, startup and shutdown.	Initially once and for new servers as and when installed

1.1.2 Server Services Management and Storage management

Along with Serves operating system, vendor will be responsible for optimum utilization, availability, reliability and security of various applications and services.
Following server applications should be managed by vendor

1) Mail Server (Zimbra Enterprise Mail Server)/DNS Server
2) I3PMS Server (IIS based Web server)
3) Web server (ITER-India webserver; RHEL, Apache)
4) PDC (Primary Domain Controller)
5) Microsoft Teams Meeting software
6) Email Anti-Spam software management
7) End point anti-virus software
8) Symantec Net Backup server
9) File server and FTP Server
10) Helpdesk software server (Web server)

Detail Scope of Work for ITER-India Mail server: This includes all necessary activities to be carried out to make server available, secure and reliable.

- Managing existing Zimbra Email server.
- Upgradation of Zimbra Email server as and when Upgrades are launched.
- Monitoring and managing Zimbra Mail server for uninterrupted email services.
- Mail traffic monitoring and proactive disk space usage for Mail.
- Problem isolation/ Trouble shooting and Resolution.
- Support for Mail related problems.
- Mail delivery management.
- Providing connectivity to remote mail users.
- Ensuring confidentiality and security of individual mail users.
- Backup of Mail data volumes.
- Generation of Mail related MIS.
- Configuring, continuously monitoring and updating SPAM filtering policy to protect users from receiving spam mails. Antispam software will be provided by ITER India and support and services shall be ensured by the vendor.
- Managing mail server for continuous availability.
- Protecting mail server from being black listed.
- Installation and Configuration of new serve if needed.

** The details of the Servers available at ITER sites have been enclosed as **Annexure A**.

Note: Server and Storage Hardware are covered under separate AMC/Warranty and is not in scope of this tender.

1.2 Network, Wi-Fi & Link Maintenance Services

Network, Wi-Fi & Link Management Services: This includes the responsibility of vendor to make sure all network components are configured and working properly to server Intranet and Internet at ITER India, Sangath and ITRE-India, Lab at IPR. The service shall cover the LAN and Wi-Fi infrastructure at ITER-India & WAN links across ITER India. This shall include following activities to be done along with any other activities required to be done, for optimum utilization of Networks and ensuring the availability of services: -

a) Weekly monitoring of LAN & WAN, using the NMS (Network Management System) Software provided by ITER-India, or monitoring through manual testing, including all the active Network components and reporting the status to ITER-India IT In-charge.

b) Configuration / Reconfiguration of Routers, Layer-2, Layer-3 switches, RAS, Hubs, Nodes, Servers etc. for Network connectivity, as and when required. Keep the back up of latest configuration of Network devices and maintaining Documentation of all updates.

c) Shall provide troubleshooting, diagnosis of switches and if needed escalating the calls to concerned vendors in case of hardware related problems.

d) Provide services for Creation and maintenance of VLAN, as per requirement.

e) Maintain an updated inventory / assets list of ITER-India IT Network Infrastructure.

f) Maintain and updated document for LAN / WAN network diagrams with relevant details for all ITER-India Locations.

g) Provide services for Protocol configuration on any new Router / Switch as per existing routing protocol.

h) Maintain and update IP address list of complete Network and optimum management of IP address. The Vendor should understand the existing IP address scheme of ITER-India and allocate the IP addresses for a new LAN segment, as per scheme.

i) Data traffic monitoring of optimum data speed for each services and performance of the Network and record keeping.

j) Overall Network performance monitoring regularly and tuning of the Network as and when required and generation of logs.

k) Provide services for implementation of Network security procedures / policy as per IT Security

Note: Network Hardware are covered under separate AMC/Warranty and is not in scope of this tender.

1.3 Disaster Recovery , Backup and Restore Service

The Scope of Services shall cover all Windows Servers, Linux Servers, for operation of Oracle business / web based applications packages in ITER-India, Security Serves, Proxy Servers, E-mail, File / print Servers & FTP SERVER etc. Following are the list of activities, to be performed by the Vendor: -

a) Perform DR, backup operations for the various Servers as per the defined backup strategy of ITER-India. This includes as is / incremental / differential backup and weekly total backup on media provided by ITER-India.
b) Conduct restoration drills with sample backed up data on a quarterly basis to confirm data integrity.
c) Maintain log sheets of backups taken.

Vendor shall generate MIS Reports on planned backup and backup actually taken on monthly basis and quarterly report on the number and success of the restoration drills.

Note: Backup device hardware are covered under separate AMC/Warranty and is not in scope of this tender.

1.4 Non-disclosure Agreement

Successful bidder shall sign a non-disclosure agreement as per Annexure-B

Annexure-A

SERVER LIST

1) I3PMS SERVER (In house Developed web application) (Only OS and web server not I3PMS application)
2) Zimbra Mail server on RHEL (VMware) (OS and Zimbra mail server)
3) Web server on RHEL (VMware)/DNS server (Both OS and Web server)
4) Active director server windows Primary domain controller.(Both OS and Domain server)
5) Antivirus server. (Both OS and Symantec Server)
6) File server, FTP server.
7) Helpdesk software server.
8) Anti-Spam Software Server.
9) VMware Vcentre severs.
10) Enovia server (Oracle server)

Hardware components

Sr.No.	Network Components	Numbers
1	Nortel BES1010-48T Switches	4
2	Checkpoint 4800 Firewall	1
3	Cisco 7200 series VXR Router	2
4	Cisco 4510+E L3 Switch	1
5	Cisco 2960 X series L2 switch	4
6	Cisco SG 300 Switch	1
7	Jack panel	12
8	RJ45 Connectors	300
9	Ruckus 7343 wireless AP	2
10	HP 5500-24G SFP El	2
11	HP 5120 24G PoE+ EI	8
12	HP MSM466 Dual Radio AP	9

Sr.No.	Servers Components	Numbers
1	Symantec NetBackup 5230	1
2	IBM DS3950 Storage	1
3	IBM DS3200 Storage	1
4	IBM DS3512 Storage	1
5	IBM V3700 Storage	1
6	IBM Blade Center H with 9 blades	1
7	IBM Blade Center E with 10 blades	1
8	IBM X 3650 Servers	3
9	IBM System Storage TS 2900	1
	HCL Servers	4

Annexure-B

NON - DISCLOSURE AGREEMENT

This Agreement made on this _____ day of ____, _____ (the **'Effective Date'**)

BETWEEN:

(1)

AND (2)

_____
_____
_____

(hereinafter referred to, individually, as the **"Party"** and collectively, as the **"Parties"**)

Background:

i) The Parties are, or will be, evaluating, discussing and negotiating a potential contractual relationship concerning the _____ _____(the **'Project'**).

ii) The Parties may, in these evaluations, discussions and negotiations, disclose to each other information that is technically and /or commercially confidential.

iii) The Parties have agreed that disclosure and use of such technical and/or commercial confidential information shall be made and on the terms and conditions of this Agreement.

Now it is agreed as follows:

1.0 Definitions:

In this Agreement the following terms shall, unless the context otherwise requires, have the following meanings:

1.1 **'Disclosing Party'** means the Party disclosing Confidential Information to the other Party under this Agreement.

1.2 **'Receiving Party'** means the Party receiving Confidential Information from the other Party under this Agreement.

1.3 **'Confidential Information'** means any information, which shall include but is not limited to, design, fabrication & assembly drawings, know-how, processes, product specifications, raw materials, trade secrets, market opportunities, or business or financial affairs of the Parties or their customers, product samples, inventions, concepts and any other technical and/or commercial information, disclosed directly or indirectly and in any form whatsoever (including, but not limited to, disclosure made in writing, oral or in the form of samples, models, computer programs, drawings or other instruments) furnished by the Disclosing Party to the Receiving Party under this Agreement.

1.3.1 Such Confidential Information shall also include but shall not be limited to:

1.3.1.1 information disclosed by the Disclosing Party in writing marked as confidential at the time of disclosure;

1.3.1.2 information disclosed by the Disclosing Party orally which is slated to be confidential at the time of disclosure;

1.3.1.3 information disclosed in any other manner is designated in writing as Confidential Information at the time of disclosure; or

1.3.1.4 notwithstanding sub-clauses 1.3.1.1, 1.3.1.2 and 1.3.1.3 of this definition, any information whose nature makes it obvious that it is confidential.

1.3.2 Such Confidential Information shall not include any information which:

1.3.2.1 is, at the time of disclosure, publicly known; or

1.3.2.2 becomes at a later date, publicly available otherwise than a wrongful act or negligence or breach of this Agreement of or by the Receiving Party; or

1.3.2.3 the Receiving Party can demonstrate by its written records was in its possession, or known to the Receiving Party, before receipt under this Agreement, and which was not previously acquired under an obligation of confidentiality; or

1.3.2.4 is legitimately obtained at any time by the Receiving Party from a third party without restrictions in respect of disclosure or use; or

1.3.2.5 the Receiving Party can demonstrate to the satisfaction of the Disclosing Party, has been developed independently of its obligations under this Agreement and without access to the Confidential Information.

1.4 **'Purpose'** means the evaluations, discussions, negotiations and execution regarding a contractual relationship between the Parties in respect of the Project defined in paragraph (i) of the **Background** section.

1.5 **'Affiliate'** means any legal entity which, at the time of disclosure to it on any Confidential Information, is directly or indirectly controlling, controlled by or under common control with any of the Parties.

1.6 **'Contemplated Agreement'** means any future legally binding Agreement between the Parties in respect of the Project envisaged under this Agreement.

2.0 Non-Disclosure of Confidential Information:

2.1 In consideration of the disclosure of Confidential Information by the Disclosing Party to the Receiving Party solely for the Purpose, the Receiving Party undertakes whether by itself, its successors and heirs, not to disclose Confidential Information to any third party, unless in accordance with Clause 4.

2.2 In addition to the undertaking in Clause 2.1, the Receiving Party shall be liable for:

2.2.1 any loss, theft or other inadvertent disclosure of Confidential Information, and

2.2.2 any unauthorized disclosure of Confidential Information by persons (including, but not limited to, present and former employees) or entities to whom the Receiving Party under this Agreement has the right to disclose Confidential Information, except where, the Receiving Party has used the same degree of care in safeguarding such Confidential Information as it uses for its own Confidential Information of like importance and in no event less than a reasonable degree of care; and upon becoming aware of such inadvertent or unauthorized

disclosure the Receiving Party has promptly notified the Disclosing Party thereof and taken all reasonable measures to mitigate the effects of such disclosure and to prevent further disclosure.

2.3 The Receiving Party understands and agrees that:

2.3.1 any information known only to a few people to whom it might be of commercial interest and not generally known to the public is not public knowledge;

2.3.2 a combination of two or more parts of the Confidential Information is not public knowledge merely because each part is separately available to the public.

2.4 The Receiving Party acknowledges the technical, commercial and strategic value of the Confidential Information to the Disclosing Party and understands that unauthorized disclosure of such Confidential Information will be injurious to the Disclosing Party.

3.0 Use of Confidential Information:

The Receiving Party is entitled to use the Confidential Information but only for the Purpose.

4.0 Permitted Disclosure of Confidential Information:

4.1 The Receiving Party may disclose in confidence Confidential Information to any of its Affiliates and employees, in which event the Affiliate and employee shall be entitled to use the Confidential Information but only to the same extent the Receiving Party is permitted to do so under this Agreement. The Receiving Party agrees that such Affiliates or employees are subject to confidentiality obligations no less restrictive than those of this Agreement.

4.2 The Receiving Party shall limit the dissemination of Confidential Information of its Affiliates and employees having a need to receive such information to carry out the Purpose.

4.3 The Receiving Party may disclose Confidential Information to its consultants, contractors, sub-contractors, agents or similar persons and entities having a need to receive such information to carry out the Purpose on the prior written consent of the Disclosing Party. In the event that the Disclosing Party gives such consents, the Receiving Party agrees that such individuals are subject to confidentiality obligations no less restrictive than those of this Agreement.

4.4 Notwithstanding Clause 2.1, the Receiving Party shall not be prevented from

disclosing Confidential Information, where (i) such disclosure is in response to a valid order of a court or any other governmental body having jurisdiction over this Agreement or (ii) such disclosure is otherwise required by law, provided that the Receiving Party, to the extent possible, has first given prior written notice to the Disclosing Party and made reasonable efforts to protect the Confidential Information in connection with such disclosure.

5.0 Copying and Return of Furnished Instruments:

5.1 The Receiving Party shall not be entitled to copy samples, models, computer programs, drawings, documents or other instruments furnished by the Disclosing Party hereunder and containing Confidential Information, unless and to the extent it is necessary for the Purpose.

5.2 All samples, models, computer programs, drawings, documents and other instruments furnished hereunder and containing Confidential Information shall remain the Disclosing Party's property.

5.3 At any time upon request from the Disclosing Party or upon the conclusion of the Purpose or expiry of this Agreement, the Receiving Party, at its own cost, will return or procure the return, promptly and in any event within 14 days of receipt of such request, of each and every copy of Confidential Information given by the Disclosing Party, and satisfy the Disclosing Party that it no longer holds any further Confidential Information.

6.0 Non-Disclosure of Negotiations:

Except as provided in Clause 4, each Party agrees that it will not, without the other Party's prior written approval, disclose to any third party the fact that the Parties are discussing the Project. The Parties acknowledge that the provisions of this Agreement shall apply in respect of the content of any such discussions. The undertaking set forth in this Clause 7 shall survive the termination of this Agreement.

7.0 Term and Termination:

7.1 This Agreement shall become effective on the Effective Date. The provisions of this Agreement shall however apply retroactively to any Confidential Information, which may have been disclosed in connection with discussions and negotiations regarding the Project prior to the Effective Date.

7.2 This Agreement shall remain in force for five (5) years from the Effective Date, except to the extent this Agreement is superseded by stipulations of the Contemplated Agreement.

7.3 The rights and obligations of each Party with respect to all Confidential

Information of the other Party that is received under this Agreement shall remain in effect for a period of five (5) years from the date of disclosure of Confidential Information.

8.0 Intellectual Property Rights:

All Confidential Information disclosed herein shall remain the sole property of the Disclosing Party and the Receiving Party shall obtain no right thereto of any kind by reason of this Agreement.

9.0 Future Agreements:

Nothing in this Agreement shall obligate either Party to enter into any further Agreements.

10.0 Amendments:

Any amendment to this Agreement shall be agreed in writing by both Parties and shall refer to this Agreement.

11.0 Severance:

If any term or provision in this Agreement is held to be either illegal or unenforceable, in whole or in part, under any enactment or rule of law, such term or provision or part shall to that extent be deemed not to form part of this Agreement, but the validity and enforceability of the remainder of this Agreement shall not be affected.

12.0 Governing Law:

This Agreement shall be governed by and construed in accordance with the laws of India and in any dispute arising out of or relating to this agreement, the Parties submit to the exclusive jurisdiction of the Courts situated at Ahmedabad, India.

13.0 General:

13.1 Upon 45 days written notice, the Disclosing Party may audit the use of the programs, materials, marketing materials, services, and such additional disclosed resources. The Receiving Party agrees to co-operate with the Disclosing Party's audit and to provide reasonable assistance and access to information.

13.2 The Disclosing Party shall not have any liability to the Receiving Party for any claims made by third parties arising out of their use of the Disclosing Party's trademarks (including "Logo") or marketing materials. The Receiving Party agrees to indemnify the Disclosing Party for any loss, liability, damages, cost or expense (including attorney's fees) arising out of any claims, which may

be made against the Disclosing Party arising out of their use of the Logo or marketing materials where such claim relates to their activities, products or services. Notwithstanding above, the Receiving Party shall have no obligation to indemnify the Disclosing Party with respect to a claim of trademark or copyright infringement based upon their use of the Logo or marketing materials, as expressly permitted under this Agreement.

13.3 The Receiving Party shall disclose of any similar agreements explicit or otherwise, for similar purpose/application with in its own organization, or any other third party.

13.4 In the event of a breach or threatened breach by the Receiving Party of any provisions of this Agreement, the Disclosing Party, in addition to and not in limitation of any other rights, remedies or damages available to the Disclosing Party at law or in equity, shall be entitled to a temporary restraining order / preliminary injunction in order to prevent or to restrain any such breach by the Receiving Party, or by any or all persons directly or indirectly acting for, on behalf of, or with the Receiving Party.

IN WITNESS WHEREOF, this Agreement was duly executed on behalf of the Parties on the day and year first above written.

For and on behalf of		For and on behalf of	
Sign	: _____	Sign	: _____
Name	:	Name	:
Title	:	Title	