



Limited Tender Enquiry (LTE)

For

**Selection of audited Cloud Service Provider (CSP) empanelled
under “Government Community Cloud Service Offerings”
category of GOI for hosting of Independent Directors’
Databank**

For

Indian Institute of Corporate Affairs
Ministry of Corporate Affairs
Government of India

Government of India / भारत सरकार
Ministry of Corporate Affairs / कॉर्पोरेट मामलों का मंत्रालय
Indian Institute of Corporate Affairs / भारतीय कॉर्पोरेट मामले संस्थान

Plot No. 6, 7 & 8, Sector – 5 / प्लॉट नंबर 6, 7 और, सेक्टर - 5
IMT, Manesar/ आईएमटी, मानेसर
Dist. – Gurgaon, Haryana / जिला – गुड़गांव, हरियाणा
PIN – 122052/ पिन – 122052

Dated: 12th March, 2025

Sub: Notice inviting Limited Tender for Selection of audited Cloud Service Provider (CSP) empanelled under “Government Community Cloud Service Offerings” category of GOI for hosting of Independent Directors’ Databank – Reg

Indian Institute of Corporate Affairs (IICA), under Ministry of Corporate Affairs, Govt. of India, invites competitive and responsive bids under two bid system (Technical & Financial Bid) from “Cloud Service Providers (CSPs) empanelled under the Government Community Cloud Service Offerings category of Ministry of Electronics & IT, GOI” for comprehensive and end-to-end hosting of a national level multitier portal (Independent Directors’ Databank Portal), as per requirement as specified in the “Scope of Work” defined in this LTE document. The Independent Directors Databank Portal has been functional since 1st December 2019 and can be referred visiting www.independentdirectorsdatabank.in

2. The complete detail regarding scope of work, eligibility conditions, evaluation process, and format for submission of technical and financial bids etc. is mentioned in this “**Limited Tender Enquiry (LTE)**” document.
3. Interested Bidders are advised to study this LTE document carefully before submitting their proposals in response to this tender Document. Submission of a proposal in response to this LTE shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications.
4. The time, date and venue details related to the proposal submission are mentioned in the “Important Information Schedule Sheet.” Proposals must be received not later than time, date and venue mentioned in the “Important Information Schedule Sheet.” Proposals that are received after the deadline will not be considered and no request for acceptance shall be entertained whatsoever. Bidder will be selected under Lowest Cost Based Selection Criteria (L1) and procedures described in this LTE.
5. **Interested, authorized and eligible Cloud Service Providers, who are duly audited and empaneled by Meity of Govt. of India for offering Cloud hosting services under the “Government Community Cloud Service offerings” category and are willing to meet the stated requirement, are requested to kindly submit their competitive bids/offers through mail to the Nodal Officer, ID Databank at niraj.gupta@gov.in.**
6. The competent authority at IICA reserves the right to amend any of the terms and conditions contained in this tender document or reject any or all the bids without giving any notice or assigning any reason thereof.

The decision of competent authority in this regard will be final and binding.

7. All the prospective bidders are requested to read and understand the terms and conditions of the contract as detailed in this LTE document before submitting their bids, as no change or alteration of the terms and conditions is permissible once the bid is accepted by this office.
8. Bidders are advised to study all instructions, forms, terms, requirements and other information in the LTE documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the LTE document with full understanding of its implications. The response to this LTE should be full and complete in all respects. Failure to furnish all information required by the LTE documents or submission of a proposal not responsive to the LTE documents in every respect will be at the bidder's risk and may result in rejection of its proposal.
9. The deadline for submission of bid is 5:00 P.M. on 02nd April 2025.
10. **For further details, bidders may contact Dr. Niraj Gupta, Nodal Officer, Independent Directors' Databank at +91- (0124)-2640195/9540100033 or through e-mail at niraj.gupta@gov.in**

Sd/-

(Dr. Niraj Gupta)
Tender Inviting Authority
IICA, M/o Corporate Affairs
Tel: 0124-2640195

Section A: IMPORTANT INFORMATION SCHEDULE

(## This is a Limited Tender Enquiry (LTE) for the Ministry of Electronics & Information Technology (MEITY) empaneled Cloud Service Providers (CSP) to provide Government Community Cloud (GCC) services for the hosting of Independent Directors' Databank ##)

#	HEAD	DESCRIPTION
1.	Name of the Purchaser	Indian Institute of Corporate Affairs, Ministry of Corporate Affairs
2.	Bid Submission Mode	The bidding documents, complete in all respects, are to be submitted to the Tender inviting authority in a sealed envelope. Sealed envelope will contain the following: a) Hard copies of technical qualification related documents; b) A Pen drive containing soft copies of documents as mentioned in point (a) without any password; and c) Another Pen drive containing encrypted PDF file (password protected) of financial bid. Password of encrypted file would be provided by the bidder, if successful in technical round, at the time of financial bid opening.
3.	Method of Selection	<ul style="list-style-type: none"> • Bidder with the lowest commercial proposal (LCS)
4.	Work Execution Schedule	<ul style="list-style-type: none"> • Maximum 7 days from the date of award of contract /issue of work order.
5.	Start date of issuance/publishing of LTE document	<ul style="list-style-type: none"> • 12th March, 2025
6.	Tender Submission Deadline	<ul style="list-style-type: none"> • 02nd April 2025 (05:00 PM)
7.	Tender Opening	<ul style="list-style-type: none"> • The tenders will be opened at 3:00 P.M. on 3rd April, 2025
8.	Tender Opening Venue	Indian Institute of Corporate Affairs, Plot No. P 6,7,8 Sec. 5, IMT Manesar, District - Gurugram, Haryana- 122052
9.	Tender Inviting Authority	<ul style="list-style-type: none"> • Dr. Niraj Gupta Nodal Officer, Independent Directors' Databank Indian Institute of Corporate Affairs, Plot No. P 6,7,8 Sec. 5, IMT Manesar District - Gurugram Haryana - 122052 Phone No.: +91-(0124)- 2640195 Email: niraj.gupta@gov.in
10.	EMD	Earnest money (EMD) of Rs. 50,000.00 (Rupees Fifty Thousand Only) in the form of bank draft in favor of Indian Institute of Corporate Affairs , payable at Manesar, Gurugram may be submitted in original through Speed Post/ Courier/ Registered Post/ By hand to the following address- Dr. Niraj Gupta Nodal Officer, Indian Institute of Corporate Affairs, Ministry of Corporate Affairs, Govt. of India Plot No. P 6,7,8, Sec. 5, IMT Manesar

		<p>District-Gurugram, Haryana PIN Code – 122052</p> <ul style="list-style-type: none"> • EMD should reach the above mentioned address before the last date/time of Bid submission. • The earnest money will be refunded to the unsuccessful bids after finalization of the contract. •
11.	Pre-Bid clarifications & meeting	<ul style="list-style-type: none"> • Prospective Bidders may submit any queries in writing by email to niraj.gupta@gov.in not later than 20th March, 2025 (by 06:00 PM). Accordingly, a pre-bid meeting will be held on 24th March 2025 at 12 Noon through video conferencing. • A VC link will be provided to bidders who submit their queries within the above-mentioned time-limit.
12.	Performance Bank Guarantee	<ul style="list-style-type: none"> • Successful bidder will have to deposit performance security money equivalent to 10% of the contract value (Purchase order value), in the shape of bank Guarantee/fixed Deposit for the period of contract. Performance Security money will be forfeited in case of violation of any of the terms and conditions of the tender or if it is found that the items supplied are not up to the mark.
13.	Language of Bid Submission	<ul style="list-style-type: none"> • Proposals should be submitted in English only
14.	Bid Validity	<ul style="list-style-type: none"> • Proposals must remain valid up to 90 (Ninety) days from the last date of submission of the Bids.
15.	Currency	<ul style="list-style-type: none"> • Currency in which the Bidders shall quote the price and will receive payment is INR only
16.	Estimated Value	<ul style="list-style-type: none"> • Rs. 45 Lakhs
16.	Name and Address for Communication and seeking clarifications	<ul style="list-style-type: none"> • Dr. Niraj Gupta Nodal Officer, Independent Directors' Databank Indian Institute of Corporate Affairs, Ministry of Corporate Affairs Govt. of India Plot No. P 6,7,8 Sec. 5, IMT, Manesar District-Gurugram - 122052 Haryana Phone No.: +91-(0124)- 2640195 Email: niraj.gupta@gov.in

Section B: Technical specification of cloud infrastructure to be offered under this LTE

Item Heading	Description	Qty.	Remarks
Internet band width	Internet Bandwidth with Dedicated Router	10	
Firewall	Dedicated Firewall with IPS	1	with minimum 2.2 Gbps IPS throughput

Production

Cloud VMs	Linux-Virtual Machine with 4 Virtual CPU, 32GB Virtual RAM, 100 GB Virtual HDD on SAS disks inside VM, CloudOS-CentOS,1IPv4IP Address	1	Portal Server Apache Tomcat
Cloud VMs	Linux-Virtual Machine with 8 Virtual CPU,24 GB Virtual RAM,500GB SSD (1500 IOPS) HDD on SAS disks inside VM, CloudOS-CentOS, 1IPv4IPAddress	1	MySQL DB Master-Salve
Staging			
Cloud VMs	Linux-Virtual Machine with 4 Virtual CPU, 16 GB Virtual RAM, 100 GB Virtual HDD on SAS disks inside VM, CloudOS-CentOS, 1IPv4IP Address	1	Portal Server Apache Tomcat
Cloud VMs	Linux-VirtualMachinewith8VirtualCPU,24GBVirtual RAM,500GB SSD (1500 IOPS) HDD on SAS disks inside VM, CloudOS-CentOS,1IPv4IPAddress	1	MySQL DB Master-Salve
Storage	Storage Capacity (Per GB) with IOPS	500	
Backup Service	Backup services (GB)	1000	
Domain	Domain registration - Public Domain	1	
SSL Certificates	Digital Certificate-Thawte SSL 123 -1 year	1	
Security Services	HIPS	15	Secure Host Protection service works together to deliver Comprehensive security
Security Services	SIEM (100EPS)	1	
Security Services	VA for Full Setup (Quarterly)	4	
Security Services	PT for web applications (Half yearly)	2	
Security Services	Audit (Quarterly)	4	
Security Services	DDOS (500 Mbps)	1	
Infra Managed services	Managed Firewall	1	24*7Support
Infra Managed services	Managed Operating System	4	24*7Support
Infra Managed services	Managed Database MySQL 8.0	2	24*7Support
Infra Managed services	Managed SIEM	1	24*7Support

Infra Managed services	Managed VA&PT	1	24*7Support
Mail Server	Dedicated	1	

Above mentioned technical specifications may be increased / decreased at the sole discretion of IICA.

Sd/-
(Dr. Niraj Gupta)
Tender Inviting Authority
IICA, M/o Corporate Affairs
Tel: 0124-2640195

Disclaimer

The information contained in this Limited Tender Enquiry document (LTE) or subsequently provided to the Bidders, whether verbally or in documentary or in any other form by or on behalf of the Purchaser or any of its employees or advisors, is provided to the Bidders on the terms and conditions set out in this LTE and all other terms and conditions subject to which such information is provided.

This LTE is not an Agreement and is neither an offer nor an invitation by the Purchaser to the Bidders or any other person. The purpose of this LTE is to provide interested parties with information that may be useful to them in the formulation of their Proposals. The information contained in this LTE has been provided to the best of knowledge and in good faith. However, the information may not be complete and accurate in all respects and may not be exhaustive. Specifically, the information regarding business processes provided in this LTE is based on the interim decisions taken by the Indian Institute of Corporate Affairs (IICA) and is expected to undergo changes in future. This LTE includes statements which reflect various assumptions and assessments arrived at by IICA in relation to the project. Information provided in this LTE is on a wide range of matters, some of which depends on the interpretation of law. The information is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law.

While reasonable care has been taken in providing information in this LTE, the Bidders are advised not to rely on this information only but also carry out their independent due diligence and risk assessments before submitting their response to this LTE. Further, the Bidders are advised to conduct their own analysis of the information contained in this LTE, carry out their own investigations about the project, the regulatory regime which applies thereto and all matters pertaining to IICA and to seek their own professional advice on the legal, financial and regulatory consequences of entering into an agreement or arrangement relating to this LTE.

The information contained in this LTE is subject to update, expansion, revision and amendment prior to the last day of submission of the bids at the sole discretion of IICA. Neither IICA nor any of its officers, employees nor any advisors nor consultants undertakes to provide any Bidder with access to any additional information or to update the information in this LTE.

IICA, its employees and advisors make no representation or warranty and shall have no liability of any nature to any person including any Bidder or Vendor under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this LTE.

Table of Contents

1.	Purpose	11
2.	Scope of Work	12
	IT infrastructure, Cloud Setup & Migration	12
	Disaster Recovery	15
	Operational Acceptance of Cloud	15
	Maintenance & Support for Cloud Services	16
	Provisioning Cloud Services for Additional Quantities	17
	Project Planning & Management	18
3.	Eligibility Criteria for CSP	22
4.	Roles & Responsibilities of Cloud Service Providers	26
	Compute Services	26
	Managed Database Services	27
	Network Services	28
	Security Services	28
	Helpdesk and Support Services	29
	Disaster Recovery Plan and Implementation	29
	Cloud Management Portal	30
	Managed Backup Solution and Services	30
	Migration Services	31
	Monitoring	31
	Reporting Services	32
	Incident Management Process and Procedures	32
	Licensing Management	33
	Proposal Preparation Cost	33
	Addendum & Corrigendum to the LTE	33
	Bid Validity Period	34
	Rights to Terminate the Process	34
	Language of Bid	34
	Right to Accept/Reject any or all Proposals	34
	Notification of Award and Signing of Contracts	34
	Failure to agree with the Terms and Conditions of the LTE	34
	Terms and Conditions of the Tender	34
5.	Bid Submission	35
	Bid Submission method	35
	Bid Submission Checklist	35
	Declaration by Bidder for not being blacklisted	35
	Bid Evaluation method	35
	Integrity Pact	38
	Non-Disclosure Agreement	43
	Cloud Services Checklist	47
6.	Draft Contract Agreement	51
	Definitions, Interpretations and Other Terms	51
	Interpretations	52
	Term of the Contract Agreement	54
	Work Completion Timelines & Payment Terms	54
	Implementation related timelines and penalties	55
	Service Level Agreements	56
	Professional Project Management	62
	Use & Acquisition of Assets during the term	62
	Security and safety	63

	Performance Bank Guarantee	64
	Indemnity	65
	Third Party Claims	65
	Warranties	67
	Force Majeure	68
	Resolution of Disputes	69
	Limitation of Liability towards IICA	69
	Data Ownership	70
	Fraud and Corruption	70
	Conflict of Interest	70
	Exit Management	71
	Termination of contract	73
	Confidentiality	74
	Miscellaneous	75
	Applicable Law	80
	Performance Bank Guarantee Format	81
7.	Annexure 1: Data Security & Privacy Requirements	83
8.	Annexure 2 - Strategic Control of Operations to be provisioned	85

Glossary of Terms

Acronym	Expansion
CSP	Cloud Service Providers
MSP	Managed Service Provider
GI Cloud	Government of India Cloud
IaaS	Infrastructure as a Service
SLA	Service Level Agreement
PC	Public Cloud
VPC	Virtual Private Cloud
GCC	Government Community Cloud
ISO	International Organization for Standardization
DR	Disaster Recovery
Meity / M/o E&IT	Ministry of Electronics and IT
GOI	Government of India
IICA	Indian Institute of Corporate Affairs
MCA	Ministry of Corporate Affairs
ID DB Portal	Independent Director's Databank Portal
NIC	National Informatics Centre
MCA-HQ	Ministry of Corporate Affairs – Head Quarter
DC	Data Centre
STQC	Standardization Testing and Quality Certification

1. Purpose

Indian Institute of Corporate Affairs (IICA) under Ministry of Corporate Affairs, GOI has been entrusted with designing, developing, deploying and managing the proposed “**Independent Directors’ Data Bank Portal**” which has been developed and launched in December 2019 to serve as a one stop online data bank cum repository for the independent directors in the country. Presently the platform has more than 35,000 individual and 3500+ corporate entities using the platform. The platform provides services for (a) registration of Independent Directors (b) registration of corporate entities to register and access the databank for the profiles of IDs (c) e learning courses through LMS (d) online self-assessment test for the registered users (e) other services such as monthly e newsletter, knowledge resources etc. which are accessed by the users of the platform. The databank has been introduced in December 2019 and is in operation with hosting on cloud server.

In this regard, IICA plans to engage a credible and reputed Cloud Service Provider (CSP) from the market for availing Cloud Services for hosting the national level databank portal. IICA intends to engage a MEITY audited and empanelled Cloud Service Provider for a period of one year initially, which may be further extended for a maximum period of another two years on a year-to-year basis, on the same rates, terms & conditions of original contract award, subject to continued satisfactory performance as per the SLA.

The following benefits are perceived by adopting a Cloud based approach:

- Availability of “IT infrastructure on demand” for hosting of the national level DB portal.
- Aggregation of IT infrastructure (Hardware, Storage and Networking) and management resources.
- Optimal utilization of IT infrastructure resources to meet individual peak loads.
- Standardization of systems: Auto-scalability, Faster implementation cycle time and Stable and predictable physical and technical environment.
- Reduced the administrative burden for IICA by avoiding the necessity of procurement, vendormanagement, addressing the technical issues etc.
- Cost based on actual usage, thus leading to reduced cost of infrastructure creation, monitoring, and management for IICA.
- Enhanced reliability and security of information system through centralized management of IT infrastructure by adopting the necessary measures and practices, such as:
 - i. Dynamic Scalability.
 - ii. Centralized and simplified management.
 - iii. Improved quality of data management.
 - iv. Lower risk of data loss.
 - v. Higher availability of system and data – 24x7x365.
 - vi. Better management of security and access control.
 - vii. Guaranteed service levels.
 - viii. Efficient and effective management of information security issues across cloud environment.

Key objectives of the project are as below-

- i. Engagement of Cloud Service Provider to maintain the cloud environment and other infrastructure
- ii. Faster Provisioning: “IT infrastructure on request” for hosting of databank as per requirements.
- iii. Greater reliability: Minimization of operational issues on account of hardware failures.

- iv. Cost Optimization: Aggregation of IT infrastructure (Hardware, Storage and Networking) and management resources at a reduced price.
- v. Optimal utilization of resources to meet individual peak loads.
- vi. Higher Security - Efficient and effective management of information security issues across cloud environment.
- vii. Standardization of systems: Auto-scalability, Faster implementation cycle time and Stable and predictable physical and technical environment
- viii. Reduced administrative burden for IICA by avoiding necessity of procurement, vendor management etc.
- ix. Making arrangement for and maintaining backup of data in cloud.

2. Scope of Work

To Provide cloud infrastructure & related services for hosting applications in the Government Community Cloud for one year with provisions for yearly extension for further two years on satisfactory performance and related review. The scope of work is as under:

- i. Managed hosting (VM instances, Storage, Security, Firewall, Anti-virus etc.)
- ii. Services like caching and searching
- iii. Storage & Backup: Backup solution including object storage & application storage
- iv. Procuring and Installation of Software licenses
- v. SSL Certificates
- vi. Bulk Emailing (cPanel)
- vii. Auto-Scaling-up and Scaling down of VM's
- viii. Network Connectivity and Bandwidth.
- ix. IaaS (Infrastructure as a Service)
- x. N/w Services: Public IPs, Network device management software
- xi. Security Services: Firewall with High Availability, Anti-virus for Windows VM
- xii. Hosting Services: Storage management, Network device management, Backup Management, & Security monitoring.
- xiii. Disaster Recovery
- xiv. Self Service provisioning Portal with API for automated provisioning
- xv. MIS and Reporting Services
- xvi. Provision of Public IPs
- xvii. Hardware Load balancing
- xviii. Connectivity to internet (NAT Gateway/Patch Server)
- xix. Adhere to Data security & privacy and future security framework envisaged for the proposed portal, refer Annexure 1
- xx. Provide strategic control during operations and maintenance, please refer Annexure 2
- xxi. Facilitate for third party VAPT audits
- xxii. Cyber Security

IT infrastructure, Cloud Setup & Migration

- i. The Bidder will be responsible for design and provisioning of required IT infrastructure as Infrastructure-As-A-Service (IaaS) & Platform-As-A-Service (PaaS).
- ii. The Bidder shall be responsible for provisioning required compute infrastructure (server/Virtual machines), storage and services.
- iii. Provision of necessary compute and storage infrastructure on the cloud including the underlying software licenses to host the application suite
- iv. Provide / configure VMs and migrate VM configurations (hardware and storage till OS level)
- v. Provision of bandwidth link required for migration of the data to the new cloud setup by

Bidder

- vi. The Bidder shall be responsible for providing required support during migration of the solution on the Cloud infrastructure.
- vii. Develop migration roadmap, identifying the constraints and inhibitors to cloud migration
- viii. Submit migration plan and related documentation
- ix. Detailed risk management plan
- x. Support in Migration of all data from existing infrastructure
- xi. The Bidder will be required to provide support for updates, upgrades, security patches etc. for software licenses. The Bidder would be required to provide enterprise level support or equivalent for software licenses, covering updates, security patches, issue resolution at software level, bug fixing etc. Bidder should inform IICA of any updates/upgrades in the software licenses before making any upgrades to the IT infrastructure provisioned on Cloud. These updates/upgrades would be tested by the application development teams on the existing application before applying and release of same in production. The Bidder shall be responsible for provisioning of Internet Bandwidth at both DC & DR and replication bandwidth between DC & DR.
- xii. Bidder will be responsible for provisioning of requisite network infrastructure (including switches, routers and firewalls) to ensure accessibility of the servers.
- xiii. The Bidder shall provide 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 hour, per day, per month and per quarter utilization reports in the desired format (excel, pdf, word etc.) based on which the payments will be made to the Bidder. Access of this monitoring tool/self service provisioning tool may be provided to IICA.
- xiv. The Bidder shall be responsible for ensuring security of overall solutions 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 such as firewall, intrusion prevention/ detection, content filtering and blocking, virus protection, event logging & correlation and vulnerability protection through implementation of proper patches and rules.
- xv. The Bidder shall offer services from DR at the time of outages in the DC. The DC & DR should work in Active-Active mode with dynamic load balancing and geographical apportionment of load. The Bidder shall be responsible for provisioning of internet 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.
- xvi. Sharing Root Cause Analysis report for any downtime or unavailability of the cloud infrastructure
- xvii. The infrastructure provisioned by the Bidder must be scalable and shall allow addition/reduction of cloud resources on demand basis.
- xviii. The Bidder will also be required to provide the following as services under the project: -
 - a. Routers, Web Application Firewall, Firewalls, Hardware Load Balancer, Bandwidth, Backup, Operations Management and Data Management

- b.** Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall,VPN, SSL, Log Analyzer, IPS, DDOS Protection)
 - c.** Reports on security breach and security related incidents along with co-relation with events
- xix. The Bidder needs to provide a solution to automatically provision the infrastructure via Self service Provisioning tool, provide metering and billing to provide service assurance for maintenance & operations activities. Detailed user level or user group level auditing, monitoring, metering, accounting etc.
- xx. Application development teams under IICA will provide the related system configurations to the Bidder for integration with Cloud Services during the deployment of the applications on cloud.
- xxi. The Cloud infrastructure and data must be maintained only at the location of the identified Cloud hosting site. Data can only be moved to other sites in case of any emergency with prior approval of the IICA. The IICA data is highly confidential and critical and therefore the data should be highly secured and must reside within India. Encryption capabilities in storage shall be required for maintaining user personal records; the bidder needs to provide the required support.
- xxii. The Bidder shall also allow application access of the Development, UAT and Production environment to the respective application development teams at IICA.
- xxiii. The Bidder will be required to provide a detailed backup solution in discussion with IICA. It is expected to provide daily backup with 28 days' retention and weekly backup with 16 weeks' retention. The Bidder shall retain information with them for 180 days after the termination of the contract, post which the provider has to wipe/purge/delete all information created or retained as part of this project.
- xxiv. The Bidder should prepare and submit a detailed implementation plan with mapping of infrastructure at DC site and DR site including following parameters:
 - a.** Server Provisioning
 - b.** Storage Requirements
 - c.** Network interfaces requirement
 - d.** Network throughput requirement
 - e.** Adequate Power and Backup requirement
 - f.** Failover mechanism for replication links
- xxv. Clock speed of the proposed VM's to be minimum 2.0 GHz Intel Xeon® E3 equivalent or higher
- xxvi. Bidder should inform about any schedule maintenance / downtime in advance (preferably 2weeks)
- xxvii. Bidder should provide NAT server / NAT Gateway with adequate Bandwidth
- xxviii. Bidder has to provide SMS and e-mail gateway services to IICA, if required and requested by IICA.
- xxix. Bidder has to provide Public IP for hosting the ID Databank Portal.
- xxx. Bidder has to provide VPN services for application access.
- xxxi. Bidder would be required to take additional data backup of entire data/incremental data on adaily basis.
- xxxii. Bidder needs to provision for FIPS 140-2 Compliant HSM for signing the Auth XML and

- decryption of e-KYC response received from UIDAI, if required and requested by IICA.
- xxxiii. Bidder should ensure the Quarterly Network Security audit by the Meity empaneled auditors.
- xxxiv. Bidder needs to ensure that application is accessible within India.

Disaster Recovery

- i. The Bidder will ensure availability of DR site within the Country.
- ii. The exact address of the Primary Site (DC) and Disaster Recovery Site (DR) will be shared by the Bidder.
- iii. The DC & DR should work in Active-Active mode. DR should be an exact replica of DC and should operate at 100% compute as DC during outages.
- iv. The Bidder shall offer services from DR at the time of outages in the DC. The Bidder shall be responsible for provisioning requisite 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.

Note:

Bidders need to provide DR as a Service (DRaaS) from a data centre located in a different seismic zone from the main DC. If a bidder is currently providing DR and DC services from the same seismic zone, such a bidder would be given a time period of 6 months to comply with the seismic zone requirement. The Bidder has to submit an undertaking regarding this in the proposal.

Operational Acceptance of Cloud

- i. Operational Acceptance shall commence once the cloud services are commissioned, and migration is completed.
- ii. Operational Acceptance will only be provided after cloud resources have been provisioned and switchover testing (as applicable) has been completed. Switchover testing would include:
 - a. Switch over of application from DC to DR as per defined RTO and RPO
 - b. Switch over applications from DR to DC as predefined RTO and RPO
 - c. Complete Data Replication and Reverse Data Replication as per RPO
 - d. Fully functional application while DR site is operational, taking into consideration the end user experience
- iii. The Bidder will have to provide the required support for conducting the Operational Acceptance Tests. Operational acceptance tests will be performed by IICA; however, CSP will have to provide the required support during Operation Acceptance.
- iv. After the Operational Acceptance has been completed, IICA will:
 - a. Issue an Operational Acceptance Certificate; or
 - b. Notify the Bidder of any deficiencies or other reason for the failure of the Operational Acceptance Tests
- v. Once deficiencies have been addressed, the Bidder shall again notify IICA, and IICA, with the full cooperation of the Bidder, shall use all reasonable endeavors to promptly carry out Operational acceptance. Upon the successful conclusion of the Operational Acceptance Tests, the Bidder shall notify IICA of its request for Operational Acceptance, IICA shall then issue to the service provider Operational Acceptance.
- vi. If the Operational Acceptance Test fails even after 3 unsuccessful attempts, then IICA may consider terminating the Contract and if the Contract is terminated the Performance Bank

Guarantee (PBG) will be forfeited.

Maintenance & Support for Cloud Services

The CSP shall be responsible for providing 24*7*365 days support for ID DB Portal Cloud infrastructure for one year from the date of issuance of operational acceptance by IICA. The project will be for a one-year contract period and may further be extended by up to maximum duration of 2 years at the same rates on a yearly basis with review of successful performance. The maintenance and support will include the following activities -

- i. Compliance process to the defined international standards and security guidelines such as ISO 27001, ISO 20000:1, for maintaining operations of cloud and ensuring privacy of IICA data.
- ii. Ensuring Uptime and utilization of the cloud resources as per SLAs.
- iii. In the event of a disaster at DC site, activation of services from the DR site is the responsibility of CSP. The CSP 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 need to be performed by the CSP half yearly to check for disaster preparedness. The CSP shall also provide a plan for handling the DR scenario including the roles and responsibilities for each stakeholder.
- iv. CSP will be responsible for providing support for software licenses at the Cloud Site for the entire contract period.
- v. On expiration / termination of the contract, CSP to hand over complete data in the desired format to the IICA which can be easily accessible and retrievable. CSP should also provide support for transitioning to other CSP.
- vi. CSP should provide provision for viewing live Dashboards for Daily report, utilization etc. through the monitoring tool/self-provisioning tool.
- vii. CSP to provide list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This has to be via an Incident Management system.
- viii. MIS Reports - CSP shall submit the reports on a regular basis in a mutually decided format. The CSP shall work out the formats for the MIS reports and get these approved by the IICA. The following is only an indicative list of MIS reports that may be submitted to IICA:
 - a. Daily reports
 - i. Summary of resolved unresolved and escalated issues / complaints
 - ii. Log of backup and restoration undertaken
 - b. Weekly Reports
 - i. Summary of systems rebooted.
 - ii. Summary of issues / complaints logged.
 - iii. Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.
 - iv. Hypervisor patch update status of all servers including the Virtual Machines running
 - c. Monthly Reports
 - i. Component wise server as well as Virtual machines availability and resource utilization
 - ii. Consolidated SLA / Non- conformance report.
 - iii. Summary of component wise uptime.
 - iv. Log of preventive / scheduled maintenance undertaken

- v. Log of break-fix maintenance undertaken
- vi. All relevant reports required for calculation of SLAs
- d. Quarterly Reports**
 - i. Consolidated component-wise availability and resource utilization
 - ii. All relevant reports required for calculation of SLAs
 - iii. The MIS reports shall be in line with the SLAs and the same shall be scrutinized by IICA
- e. Six monthly reports on VA/PT and other security related areas.**

Provisioning Cloud Services for Additional Quantities

- i. Indicative quantities and compute for IT Infrastructure components for availing cloud services are mentioned in the LTE. This is an indicative sizing against which the Bidder will be commercially evaluated. The actual sizing will be provided for the Bidder after on-boarding.
- ii. The bidder is required to provision at least 25% of the indicative demand proposed to be achieved at the end of 1 year, at the time of operational go live. The subsequent enhancements required will be assessed by IICA on a monthly basis and indicated 10 days in advance of each quarter.
- iii. The rates offered for cloud services must be valid for entire contract/project duration. No variation in these quoted rates shall be allowed for a one-year contract period which can be further extended by up to a maximum of two years at the same rates on a yearly basis.
- iv. IICA reserves the right to scale down and scale up the IT infrastructure. The payment would be made only on the actual usage of the IT infrastructure as per the rates provided by the Bidder in the Commercials.
- v. In addition to these services, Bidder to provide the following access to IICA and concur with the following requirements: -
 - a. Access to cloud management portals/self service provisioning tool
 - b. Ability to add/delete compute and storage resources
 - c. Ability to create, edit and delete VMs
 - d. Root access on all VMs
 - e. Provide access to utilization reports and audit trail on cloud
 - f. Provide access to monitoring dashboards
 - g. Full management access on cloud all accounts, full root access on all VMs
 - h. API to create, configure and delete VMs
 - i. Provide Fully reliable binary object storage service
 - j. Provide Web Console access to VMs
 - k. Ability to add storage to VMs without restarting the VMs
 - l. VM utilization reports and recommendations
 - m. High speed read and write access to backup storage
 - n. CSP should provide root cause analysis of all non-application issues
 - o. Bulk Data import feature for migrating via disks
 - p. Bulk data export feature

Project Planning & Management

The success of the project depends on the proper planning and management of the project. At the

onset, Bidder shall plan the project implementation in great detail and should provide a micro level view of the tasks and activities required to be undertaken in consultation with the IICA. An indicative list of planning related documentation that the Bidder should make at the onset is as follows:

- i. **Project Schedule:** A detailed week-wise timeline indicating various activities to be performed along with completion dates and resources required for the same.
- ii. **Workforce Deployment List:** A list needs to be provided with resources that will be executing the project along with the roles and responsibilities of each resource.
- iii. **Resource Deployment List:** List and number of all cloud-based resources (including but not limited to servers (VMs), storage, network components and software components) other than workforce that may be required.
- iv. **Communication Plan:** Detailed communication plan indicating the form of communication, kinds of meeting along with recipients and frequency.
- v. **Migration Plan:** The Bidder will be required to submit a migration plan for migrating AB-NHPM on cloud. Necessary support will be provided by IICA in conjunction with application development teams.
- vi. **Backup Solution and Plan:** Bidder will be required to clearly provide details of their Backup solution and detail out plan to take data backup.
- vii. **Adherence to SLAs:** The Bidder is required to adhere to all SLAs as per the LTE.
- viii. **Progress Monitoring Plan and Reporting Plan:** Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will be approved by the IICA to the successful bidder before the start of the project.
- ix. **Standard Operating Procedures:** Detailed procedures for operating and monitoring the Cloud site.
- x. **Risk Mitigation Plan:** List of all risks and methods to mitigate them.
- xi. **Escalation Matrix & Incident Management:** A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This has to be via an Incident Management system.
- xii. **Exit Management and Transition Plan:** A detailed exit management and transition plan outlining details and activities to be undertaken in case of termination of contract or in case of completion of contract period.
- xiii. **Disaster Recovery Plan:** A detailed plan for seamless change-over from the DC to the DR during outages needs to be provided.

Further, the CSP is required to and shall ensure the following:

a. Security Solutions

- i. The bidder should be able to provide **Managed SIEM + Managed WAF + Server Security + managed DDoS Detection & Mitigation Service** Solution to take care of overall Security requirements.
- ii. The cloud based Managed DDoS Detection & Mitigation Service should ensure the Application Availability of IICA'S critical Application from Denial of Service types of attacks.
- iii. Bidder should have a Service Operations Centre (SSOC) to provide 24/7 real-time security monitoring, alerting, and reporting capabilities, through their trained certified security specialists for the proposed Services.
- iv. Cloud Security Audit Services: Supplier will Identifying the potential security vulnerabilities. how to prevent future attacks using audit tools. Suggest and develop strategies for protection from attacks and take measures against potential failures, by using trending security and monitoring tools with proficient automation.

b. SIEM

- i. The cloud SIEM solution provided by the bidder should provide security visibility across all Servers and security infrastructure.
- ii. The proposed SIEM solution shall consist of Loggers, Collectors and Co-relation Engine.
- iii. A maximum of 100 EPS log processing capacity should be considered in the current solution, however it can be upgraded with change request.
- iv. The connectors deployed at the Cloud node should be capable of collecting OS logs from VMs and the logs from proposed security devices, further the connectors should compress and encrypt the logs before sending them over MPLS link.
- v. Bidder's SOC should provide 24/7 monitoring through SIEM

Scope of Work:

Indicative Scope Of Work	
Bidder's Scope of Work – SIEM	
1	Bidder to manage and monitor the connector applications at DC+ DR.
2	Bidder shall define creating correlation rules based on customer devices
3	Bidder will manage and monitor log management, reporting and alerts.
4	Based on the report findings, Bidder shall provide the log and finding analysis.
5	Bidder will provide 24x7 technical help providing L1, L2 and L3 remote SSoC support for SIEM Incident Management.
6	Periodic reporting shall be scheduled and sent out as email reports.
7	Bidder shall provide the dashboard through SIEM Solution and reports can be downloaded by customer and read only access will be provided to customer.

c. Proposed Solution Managed DDoS Detection & Mitigation Service

- i. Bidder needs to provide Cloud based DDoS Solution to protect IICA's environment hosted at the Government Community Cloud
- ii. Bidder will provision separate sub-interface for GRE tunnels on the managed Router for IICA's (initiated from Scrub farm to deliver clean traffic in event of DDOS attack) at the

- Cloud node.
- iii. All DDoS mitigation takes place within Bidder`s backbone, and all attack traffic is mitigated in the cloud before it reaches the Customer premises.
- iv. The flow information is automatically collected from Bidder`s routers and fed into DDoS service. As a part of the initial deployment, the traffic was benchmarked, and this traffic benchmark was used to identify sudden changes in traffic pattern.
- v. DDoS service from Bidder detects different kinds of DDoS attacks including traffic pattern-based attack detection and traffic signature-based attack detection.
- vi. If a DDoS attack is detected, the mitigation component of DDoS Service routes traffic to DDoS mitigation devices, where the DDoS attack packets are identified and dropped. The valid traffic is passed to the Customer over GRE tunnel.
- vii. The DDoS Detection and Mitigation service provides customers with a managed and shared system for analysis, identification, reporting, alerting and mitigation of anomalies in Internet traffic.
- viii. Mitigation is manually started and there is no automatic way of doing mitigation. Also, online mitigation via Portal is not supported. Detection and Mitigation Turnaround time will be done within 10 Minutes.
- ix. Bidder will Detect the below types of DDoS attacks thorough DDoS detection & mitigation Service

1. Misuse Type

- a. Chargen Amplification
- b. DNS Amplification
- c. ICMP Flood
- d. IPv4 /IPv 6 Protocol
- e. IP Private Misuse
- f. MS SQL RS Amplification
- g. NTP Amplification
- h. SNMP Amplification
- i. SSDP Amplification
- j. TCP null
- k. TCP RST
- l. TCP SYN
- m. UDP Flood

d. Reporting

mDDoS Detection and Mitigation Service customers are provided with secure web-based access to the Bidder Security Service portal from which a variety of functions can be performed.

The following reporting functionality is provided by the Security Service portal:

- i. Alert summary
- ii. Traffic summary
- iii. TCP and UDP protocol traffic summary
- iv. Top IP “talkers” summary

Scope of Work

Indicative Scope Of Work	
Bidder Scope of Work	
1	Bidder will configure GRE Tunnel [FCS - Please share the context of this requirement]
2	Bidder is responsible for installation, configuration and troubleshooting of GRE Tunnel, created for sending clean traffic during mitigation for Bidder managed CPE
3	Bidder shall provide Monitoring Portal with portal Access
4	Bidder will provide standard test plan guide for GRE Testing

e. Service Level Agreements

- i. Cloud DDoS Service SLA include
- ii. Service availability guarantee for scrubbing device(s)
- iii. Service activation.
- iv. Administrative changes
- v. DDoS attack notification guarantee
- vi. Time to mitigate guarantee

f. Service availability guarantee for scrubbing device(s): Bidder needs to provide service availability guarantee for the scrubbing device(s) as determined by the availability of the scrubbing devices and the platform, to mitigate DDoS attacks.

g. Server Security

- i. Anti-virus and HIPS solution is deployed for protecting IICA'S Windows & Linux Servers at GCC.
- ii. The signature files are updated on the managed servers daily by the Antivirus Management Server. The Antivirus software is configured to scan the full system once and a real-time active scan is enabled to clean or quarantine any virus infected files in the systems. Folders or files exclusions may be configured.
- iii. When servers are infected by a virus, the antivirus agent triggers an alert to the console and the Bidder's operations team receives an email alert triggering an action. IICA's are notified when the server file is infected by a virus. The quarantine folder is cleaned up on consecutive release of updates or automatically after 30 days.
- iv. A single-pane console consolidates security policy and management across DC & DR servers for Anti-Virus, HIPS & Application control. Bidder proposes Server Security which Leverage defense optimized specifically for virtual instances to avoid resource storms that can strain underlying infrastructure.

- v. Volumetric considered: Anti-Virus and HIPS:
- vi. Key Benefits:
 - i. Virtual Machine-optimized threat defenses deliver multilayer countermeasures.
 - ii. Centralized management and automated workflows drastically reduce complexity
 - iii. Gain multi-layer protection from advanced malware and intrusion with ease of use.
 - iv. Visualize and discover network threats without installing an agent.
 - v. Secure your environment by taking corrective actions directly from within the solution.

h. WAF (Web Application Firewall)

- i. Bidder needs to provide WAF services for IICA’S Web Applications hosted at Bidder GCC
- ii. Bidder needs to provide Web Application Firewall (WAF) for delivering the Web application security services to secure Web Applications from the Internet threats, hosted in dedicated instance in physical or virtual appliance.
- iii. Bidder’s WAF services will be provisioned in the Reverse Proxy mode of deployment
- iv. This deployment mode provides the highest security as all traffic is terminated in WAF; all TCP connections are accepted by WAF and are only forwarded to the protected web server following a security policy compliance inspection.
- v. The traffic should be source NATted so that the return traffic also gets inspected and protected by the WAF.
- vi. Bidder’s SLAs guarantee performance metrics should cover change management, threat signature updates, availability and reporting.
- vii. A minimum concurrency of 1000-1500 users should be there all the time.

i. VAPT and Audit: -

Bidder shall perform regular security assessments (every quarter) for the infrastructure managed by CSP and share the relevant report with IICA’s. Further, IICA’s may also get security assessments conducted through external agencies. High risk security vulnerability shall be patched within 5 days of reporting vulnerability, whereas Medium risk security vulnerability shall be patched within 15 days of reporting.

3. Eligibility Criteria for CSP

- i. Only the CSPs, empaneled by MEITY and notified on the MEITY website as on the bid submission date, for providing the following cloud services in a GCC environment shall be eligible to bid for this project:

Sl. No.	Description of Cloud Service	Whether empaneled with Meity, with full compliance (Yes/No)
1.	Infrastructure as a Service (IaaS)	
2.	Platform as a Service (PaaS)	

3.	Disaster Recovery as a Service (DRaaS), with the DR site located in a different seismic zone.	
4.	Dev/Test Environment as a Service	
5.	Managed services: Backup services	
6.	Managed services: Disaster Recovery and Business Continuity Services	

ii. The Bidder shall be responsible for meeting all obligations and the delivery of products and services mentioned in this LTE. The Bidder would also be responsible for ensuring the successful execution proposed solution including meeting the SLAs.

The Bidder will be responsible for:

- The supply, delivery and installation of all products and services mentioned in the LTE.
- Operating and maintaining the Helpdesk services for the time mentioned in the LTE.

iii. It is the responsibility of the Bidder to ensure that it is compliant with all the clauses as mentioned in the bid, failing which bid can be disqualified.

iv. All the information requested for pre-qualification shall be provided by the bidding firm. Failure to provide information, which is essential to evaluate the bidder's qualification, or to provide timely clarification or substantiation of the information supplied may result in disqualification of the bidder.

v. Pre-qualification will be based on meeting all the following minimum criteria regarding the bidder's general and special experience, personnel, equipment and financial capabilities, as demonstrated by the bidder's responses in the forms attached.

vi. The bidder should satisfy the criteria below and should invariably submit valid documentary evidence through the standard process of LTE to support the eligibility claim:

#	Criteria	Description	Documentary Evidence
1	<u>Registration</u>	The CSP, as a single legal entity (Company), must be incorporated and registered in India under the Indian Companies Act 1956/2013 or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008	<ul style="list-style-type: none"> i. Copy of Certificate of Incorporation or Certified copy of Partnership Deed. ii. GST Registration Certification
2	<u>Certificate</u>	The Cloud Service Provider must be empanelled with M/o Electronics & IT of GOI under "Government Community Cloud Service Offerings" category.	Proof of valid Empanelment by Meity (reference on Meity website or Empanelment Certificate).

3	<u>Blacklisting</u>	The CSP should not have been debarred or blacklisted by any Central Government Ministry, Department, Attached Office, Subordinate office, Statutory Body, Regulatory Body, Central University, Autonomous Body, CPSEs or State Government Department, Attached Office, Subordinate office, Regulatory Body, State University, Autonomous Body, State PSEs.	The bidder shall provide a certificate with the bid that the firm and OEM have not been debarred/ blacklisted for any reason for any period by any agency mentioned above during the last 5 years. If so, particulars of the same may be furnished. Concealment of facts shall not only lead to cancellation of the bid/order but may also warrant legal action. Bidder debarred/ blacklisted by any Central Government Ministry, Department, Attached Office, Subordinate office, Statutory Body, Regulatory Body, Central University, Autonomous Body, CPSEs or State Government Department, Attached Office, Subordinate office, Regulatory Body, State University, Autonomous Body, State PSEs as on bid calling date for non-satisfactory past performance, corrupt, fraudulent or any other unethical business practices shall not be eligible.
5	<u>Certification & Compliance</u>	The CSP should be ISO certified/possessing quality certification and compliance. 1. ISO 9001:2015 or above (Certificate) 2. ISO 27001:2013 or above (Certificate) 3. ISO 27017:2015 (Certificate / Compliance) 4. ISO 27018: 2014 or above (Certificate/ Compliance) 5. SOC 1 and SOC 2	Copies of valid certificate issued to the CSP
6	<u>Resources</u>	The SP must have at least 100 IT professionals in Cloud computing for 24x7 management of different technology domains with L1, L2 and L3 skills. <ul style="list-style-type: none"> • Compute • Storage • Network • Cloud Security • Platforms (Database, Middleware, .Net, Java etc.) 	List of resources with name, designation, role, duly certified by the authorized signatory on official letterhead of the CSP.

7	<u>Experience</u>	<p>i. The CSP should have provided Cloud services at the CSP's Data centre in India for a minimum period of three completed years as on the date of submission of the bid i.e., in the year 21-22, 22-23, 23-24.</p> <ul style="list-style-type: none"> The bidder should have carried out at least 3 assignments in the aforesaid duration of a minimum work value of Rs.1 Cr each for the similar scope of work. <p>ii. The CSP should have experience of working with at least one Government Institution in the last three years for a minimum period of 2 years.</p>	<p>i. Purchase Orders /Work Orders / Contract Agreement indicating contract value, scope & period.</p> <p>ii. Successful service certificate from the Client(s).</p> <p>iii.</p> <ul style="list-style-type: none"> Work Order + Self Certificate of Completion/Ongoing (Certified by the Statutory Auditor/Company Secretary). <p style="text-align: center;">AND</p> <ul style="list-style-type: none"> Contract clearly highlighting the Scope of Work, Bill of Material and value of the Contract/order OR Self-certificate from the CSP mentioning the Scope of Work, Bill of Material and value of the Contract/order, signed by Statutory Auditor/Company Secretary of the Bidder for this bid
8	<u>Empanelment</u>	The bidder should be empanelled as a Govt. Community Cloud Service Provider with Ministry of Electronics and Information Technology (MEITY), Govt. of India and STQC audit compliant.	<p>i. Certificate of empanelment with Ministry of Electronics and Information Technology, Gol.</p> <p>ii. STQC audit compliance certificate.</p>
9	<u>Operational Data Centre</u>	The CSP must be operating at least two (2) Data Centre / Disaster Recovery Centre Facilities in India at time of submission of the bid where the Government Community Cloud should be operational. Proposed DR site should be in different seismic zone (within India).	Self-certificate from the CSP mentioning the location details signed by authorized signatory of the CSP for this bid
10	<u>Centralized NOC</u>	CSP should have a dedicated NOC (Network Operation Centre) and Business continuity plan/location (BCP) in place	Yes/No location details to be provided

11	Centralized SOC	CSP should have a dedicated SOC (Security Operation Centre) and Business continuity plan/location (BCP) in place	Yes/No location details to be provided
----	------------------------	--	--

4. Roles & Responsibilities of Cloud Service Providers

The overall roles and responsibilities of a Service Provider includes but not limited to - study of existing user department setup (if applicable), establishing connectivity between User Department's premise to Cloud DC and DR site, migration of existing applications / data to Cloud and vice versa, deploying new applications on Cloud, user administration, security administration, planning and implementation of Cloud Management and Monitoring Portal for complete infrastructure and services procured, setting up of DR site (if applicable), monitoring & reporting, exit management, billing management, etc.

It may be noted that all roles and responsibilities specified in the CSP Empanelment LTE / Application are under the scope of the Service Providers defined in this document. The roles and responsibilities of a Service Provider in each category of Cloud services are specified below. Please note that these are just the indicative list of roles and responsibilities. User Departments may specify their own set of requirements.

Compute Services

The Compute Services are the basic components of IT Infrastructure that can be used by the User Departments to run their variety of workloads such as compute-intensive workload, memory intensive workload, general-purpose workload, etc. using Virtual Machines and or Containers.

The overall roles & responsibilities of a CSP on providing VMs and Containers are including but not limited to:

- i. Provisioning of Virtual Machines
- ii. Installation, Configuration, Commissioning/De-commissioning and Management of the Virtual Machines and provide User Department the access to the same via secured web browser / Command Line Interface
- iii. Migration of Virtual machines (Physical to Virtual / Virtual to physical / Virtual to Virtual)
- iv. Monitor VMs up/down status and resource utilization such as RAM, CPU, Disk, Processes etc.
- v. Management of the OS processes and log files including security logs retained in guest VMs
- vi. Antivirus, Anti Malware, Anti Ransom ware protection
- vii. Vertical and Horizontal scaling UP/ Down of VMs
- viii. Any other activity associated with operations and management of Compute Services

Storage Services

The Storage services can be defined in various categories Object Storage, File Storage, Block Storage, and Archival Storage. The Managed Storage Services is a storage infrastructure that is provisioned keeping the user needs in mind. The roles & responsibility of a SP include but are not limited to: - ☐

- i. Scalable Storage Capacity is provisioned as per requirements and availability of resources
- ii. The SATA / SAS / SSD disks shall be made available to the User Departments, meeting the iops

- requirement
- iii. The provisioning, configuration, management, maintenance and support of storage devices shall be done by the SP
- iv. Create and Assign storage LUNs over the SAN to the managed server
- v. Any other activity associated with operations and management of Storage Services

Managed Database Services

The Managed Database Service under Cloud Service Provider (CSP) roles & responsibilities, include but not limited to,

Basic DBA Services

- i. Installing, configuring and upgrading database server software
- ii. Setting up databases
- iii. Managing database servers
- iv. Starting up and shutting down database instances¹
- v. Scheduling jobs for the databases hosted
- vi. Creating databases and environments
- vii. Controlling and supporting migrations
- viii. Supporting and troubleshooting all database issues on a 24x7x365 basis
- ix. Proactive Database Monitoring
- x. Verifying that all instances are running
- xi. Looking for any new alert log entries for errors
- xii. Looking for trace files
- xiii. Monitoring sessions, activity/redo logs, replication/standby status and objects
- xiv. Verifying free space in table spaces
- xv. Verifying rollback segments
- xvi. Performance Management – Measure taken when there is a customer need/issue
- xvii. Verifying that server has enough resources for acceptable performance
- xviii. Tuning performance as needed
- xix. Monitoring database growth and refreshing statistics weekly
- xx. Generating monthly reports on database health
- xxi. Identifying bad growth projections

- xxii. Identifying space-bound objects
- xxiii. Reviewing contention for CPU, memory, network, and disk resources
- xxiv. Reviewing fragmentation by investigating row chaining and other areas of fragmentation
- xxv. Implementing and maintaining a reliable database environment

A reliable database environment is maintained through following activities-

- i. Implementing database failover technology
- ii. Ensuring minimum committed SLA uptimes on the database environment
- iii. Establishing privileges and access controls
- iv. Managing vendors.
- v. Resolving database incidents, errors and corruption
- vi. Database Alerts and monthly reports (CPU overload, RAM memory overload, Trace and Dump file, alert log message, low free space in archive redo log directory)
- vii. Database Backup and Recovery

Network Services

The scope of the Cloud Service Provider (CSP) shall include but not limited to,

- i. Maintain and manage the required networks components for the Cloud Services procured by the User Department.
- ii. Establishing, monitoring and management of Network Connectivity from User Department to Cloud DC and Cloud DR site.
- iii. Configuration and Management of Virtual Networks, Subnets, Layer 4 / Layer 7 Load balancer, DNS
- iv. Network Monitoring, Alerting & Reporting
- v. Installation, configuration, management, monitoring and testing of Virtual / Physical Firewall
- vi. Any other activity associated with operations and management of Network Services

Security Services

The scope of the Cloud Service Provider (CSP) shall include but not limited to,

- i. Provisioning, Installation, Configuration, Management, Monitoring of Security Services as per the requirements of User Departments.
- ii. Maintain and manage access control with Network Security Groups, NACL and routing tables
- iii. Identifying Security Configuration gaps

- iv. Provision, manage and deploy HSM (High Security Module) as per User Department(s) requirement
- v. Implementation of tools such as IPS, IDS, SIEM
- vi. Conduct Security / Risk Assessment
- vii. Implementation of Multi-Factor Authentication Services
- viii. Comprehensive Application security
- ix. Implementation, management and monitoring of DDoS, IPS, IDS technology and solutions to ensure the security of Cloud Services procured
- x. Installation, Configuration, Implementation and management of Log Analyzer
- xi. Deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with a higher security layer
- xii. Cloud offering should have built-in user-level controls and administrator logs for transparency and audit control.
- xiii. Provisioning, Installation, Configuration, Management and testing of anti-virus including anti-malware, anti-spyware, ransom ware protection tools etc., investigate incidents, and undertake remedial action necessary to restore servers and operating systems to operation.
- xiv. Deploy security patches on hardware and software
- xv. Take regular backups of security configurations
- xvi. Any other activity associated with operations and management of Security Services

Helpdesk and Support Services

The scope of the Cloud Service Provider (CSP) shall include but not limited to,

- i. Create and maintain a Helpdesk / telephonic number and email based ticketing system that will resolve problems and answer queries related to the work order. The help desk support for users shall be provided on 24 x 7 x 365 basis over telephone, chat and ticketing system.
- ii. Helpdesk and Technical support services to include system maintenance support windows
- iii. Implement the monitoring System including any additional tools required for measuring and monitoring each of the Service Levels as per the SLA between the Government Department and the CSP
- iv. Provide support for 3rd party audits – enable logs and monitoring as required
- v. Defining Auto-scaling rules and limits
- vi. Providing reports for resource utilization and auto scaling
- vii. Provisioning of Incident monitoring & tracking system using web interface
- viii. Any other activity associated with operations and management of helpdesk and Support Services

Disaster Recovery Plan and Implementation

The scope of the Cloud Service Provider (CSP) shall include but not limited to,

- i. Setup and configuration of VMs, Storage, Network, Database, etc. at DR site meeting RPO and RTO requirements of the User Department
- ii. Replication tools and mechanism between DC and DR site
- iii. Network connectivity from User Department to DR site
- iv. DR drills should be conducted once every six months
- v. Define the procedure for announcing DR based on the proposed DR solution.
- vi. Clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR.
- vii. Plan the activities to be carried out during the Disaster Drill and issue a notice to the Department at least 15 working days before such a drill.
- viii. RPO monitoring, reporting and event analytics for disaster recovery solutions
- ix. Automated switchover/ failover facilities (during DC failure & DR Drills).
- x. Any other activity associated with operations and management of DR Plan and Implementation

Cloud Management Portal

The scope of the Cloud Service Provider (CSP) shall include but not limited to,

- i. CRUD Operations: MSP to Create, Read, Update, Delete, users based on roles & rights defined by User Department
- ii. Preparing Monitoring Reports
- iii. Preparing SLA Reports
- iv. Preparing Backup Reports
- v. Preparing VMs Status report
- vi. Provisioning /De-provisioning of VMs
- vii. Creating templates for VMs
- viii. Make changes in configurations for user administration
- ix. Any other activity associated with operations and management of Cloud Management Portal

Managed Backup Solution and Services

The scope of the Cloud Service Provider (CSP) shall include but not limited to,

- i. Full Server Backup of Virtual Machines including Bare Metal recovery, System States Backup, Disk Drive Backup, Folder & File level Backup, Volume Shadow Copy and Snapshots of VMs.
- ii. Database Backup with DB and its logs for all the Database Servers supporting to such as, Microsoft SQL, MySQL, Enterprise DB / Postgre SQL, Oracle, MySQL, etc.
- iii. Non-database files include PDF, XLS, XLSX, JPEG, MP4, DWG, etc. and other similar flat files.
- iv. Application Aware Backup
- v. Monitoring all Backup Jobs and their reporting
- vi. Incident Management for all backup jobs getting failed

- vii. Disk / Tape based backup as per User Department requirements
- viii. Backup Cycle and retention as per User Department requirements / backup policy
- ix. Backup and recovery of Virtual Machines, files and folders, configuration and scheduling of backups through centralized web based console
- x. Any other activity associated with operations and management of Managed Backup Solution and Services

Migration Services

The scope of the Cloud Service Provider (CSP) shall include but not limited to,

- i. Provide migration services to the User Department for migration of VMs, data, content, applications from existing setup to Cloud solution procured or existing Cloud service provider to another Cloud service provider or User Departments Infrastructure, as required by the department
- ii. Deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with a higher security layer
- iii. Rectify the problems with respect to migration of the User Department applications and related IT infrastructure including installation/reinstallation of the system software etc.
- iv. Provide Physical to Virtual and Virtual to Virtual migration from existing setup to Cloud DC-DR setup
- v. Any other activity associated with operations and management of Migration Services

Monitoring

The scope of the Cloud Service Provider (CSP) shall include but not limited to,

- i. Deploy agent based monitoring for Cloud infrastructure monitoring
- ii. Monitoring performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications, including API access
- iii. Monitor Internet links, Replication links, MPLS, P2P (as applicable), including but not limited to Bandwidth utilization, Data transfer, Response time (latency) and Packet loss.
- iv. Monitor daily, weekly, monthly backup jobs as per schedule and during any unsuccessful backup the incident management process and procedures should be invoked.
- v. To perform regular health checks of VMs, Storage, N/w links, etc.
- vi. Reviewing the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels
- vii. Implement necessary tools to monitor the root cause for performance degradation of any applications. User Department should be able to analyze whether the issue is actually an Application issue or Hosting/hardware/Bandwidth issue.
- viii. Investigate outages; perform appropriate corrective action to restore the hardware, software, operating system, and related tools
- ix. Investigate outages; perform appropriate corrective action to restore the hardware, software

- x. Any other activity associated with Monitoring Services

Reporting Services

The scope of the Cloud Service Provider (CSP) shall include but not limited to,

- i. Track system usage and usage reports
- ii. Provide relevant reports including real time as well as past data/information/reports for user Departments
- iii. Summary of resolved unresolved and escalated issues / complaints
- iv. Logs of backup and restoration undertaken report
- v. Component wise Virtual machines availability and resource utilization report
- vi. Consolidated SLA / Non- performance report
- vii. Any other activity associated with Reporting Services

Incident Management Process and Procedures

The scope of the SP shall include but not limited to,

- i. Adhere to ITIL V3 (latest) guidelines and process for incident, problem and change management.
- ii. Activate Incident management teams(s) for any high severity incident or as agreed by the User Department
- iii. Any other activity associated with Incident Management Process and Procedures

- a. Problem Management

When repeated correlated incidents occur, or when a workaround has been initiated to rectify an incident, Supplier reviews the incidents to determine whether the incidents should be classified instead as problems. If identified as problems, Supplier initiates the Problem Management process to further investigate, track, identify and correct problem root cause. Customers are notified of any identified problems via the monthly Service report, described in the Service Level Management section of this document.

- b. Configuration Management

Supplier maintains asset records of all significant components used to provide the Service. The asset records relating to the Service(s) to which Customer has subscribed can be made available to Customer upon request for audit purposes.

- c. Capacity Management

Supplier is responsible for ensuring enough capacity is available to meet the requirements of the Service(s) set forth on the BOQ. Customer is responsible for regularly tracking capacity of the Services and reporting initial and ongoing capacity requirements to Supplier. Capacity Management information for the Service is available to Customers through the technology portal and monthly Technology Reports provided to Customer by Supplier.

- d. Change Management

Supplier may be required to make changes occasionally to the IT infrastructure used to provide the Service(s) in order to correct problems or meet other requirements, such as, but not limited to, fulfilling a Customer's request or installing a required patch. When a change is required, Supplier assesses the feasibility of the change through a Change Advisory Board process and, if approved, classifies the change per the table below

e. Service Level Management Reports

1. Supplier delivers Service Level Management Reports to Customer that demonstrates the performance of the Service against the agreed Service levels described in this document.
2. Incidents raised or carried forward, including severity and time to resolution
3. Problems raised or carried forward
4. Requests initiated by Customer
5. Changes carried out to hardware, software and tools in line with the Service provided to Customer
6. Actual Service availability achieved (percentage)

Licensing Management

The scope of the CSP shall include but not limited to,

- i. The Cloud Service Provider shall be responsible for migrating the existing OS, Database, Backup, Antivirus licenses etc. (if applicable as per License agreement with the OEM) on Cloud
- ii. Management of licenses in Cloud environment
- iii. Any new licenses offered to the User Department shall abide by OEM Terms & Conditions of Licensing agreement
- iv. The Cloud Service Provider shall be responsible to procure any 3rd part license on behalf of User Department, as desired and permitted by the department
- v. Any other activity associated with operations and management of existing or newly procured licenses

Proposal Preparation Cost

The bidder is responsible for all costs incurred in connection with participation in this process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal, in providing any additional information required by IICA to facilitate the evaluation process, and in negotiating a definitive Contract or all such activities related to the bid process. IICA will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process. All materials submitted by the Bidder shall become the property of the IICA and may be returned at its sole discretion.

Addendum & Corrigendum to the LTE

At any time prior to the deadline for submission of bids, IICA may, for any reason, modify the Bid Document by an amendment. All the amendments made to the document would be informed by all the participating agencies through e-mail. IICA also reserves the right to amend the dates mentioned in this Bid Document for bid process. IICA may, at its discretion, extend the last date for the receipt of Bids.

Bid Validity Period

- Bid shall remain valid for the time mentioned in the “Important Information Schedule.”
- IICA may request the Bidder(s) for an extension of the period of validity.

Rights to Terminate the Process

IICA may terminate the LTE process at any time without assigning any reason. IICA makes no commitments, express or implied that this process will result in a business transaction with anyone. This LTE does not constitute an offer by IICA. The bidder's participation in this process may result in IICA selecting the bidder to engage in discussions and negotiations toward execution of a contract. The commencement of such negotiations does not, however, signify a commitment by the IICA to execute a contract or to continue negotiations. IICA may terminate negotiations at any time without assigning any reason.

Language of Bid

The Bids prepared by the Bidder and all correspondence and documents relating to the bids exchanged by the Bidder and IICA, shall be written and communicated in English language.

Right to Accept/Reject any or all Proposals

IICA reserves the right to accept or reject any proposal, and to annul the bidding process and reject all Bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected bidder or bidders of the grounds for IICA's action.

Notification of Award and Signing of Contracts

Prior to the expiration of the period of proposal validity, the Bidder will be notified in writing or by fax or email that its proposal has been accepted. IICA shall facilitate signing of the contract after the notification of the award. However, it is to be noted that the date of commencement of the project and all contractual obligations shall commence from the date of issuance of Work Order/Letter of Acceptance or date as decided by IICA, whichever is later. All reference timelines as regards the execution of the project and the payments to the Bidder shall be considered as beginning from the date of issuance of the Work Order/Letter of Acceptance or date as decided by IICA, whichever is later. The notification of award (Work Order/LOA) will constitute the formation of the Contract. Upon the Bidder executing the contract with IICA, it will promptly notify each unsuccessful Bidder. After issuance of Work Order/LOA the Bidder shall sign the Contract as per the draft contract format given in the LTE.

Failure to agree with the Terms and Conditions of the LTE

Failure of the bidder to agree with the Terms and Conditions of the Bid shall constitute sufficient grounds for the annulment of the contract. The contract may be awarded to the next most responsive bid of another Bidder.

Terms and Conditions of the Tender

Bidder is required to refer to the Draft Contract Agreement, in this LTE Document, for all the terms and conditions (including project timelines) to be adhered by the successful Bidder during Project

Implementation and Post implementation period.

5. Bid Submission

Bid Submission method

The bidding documents, complete in all respects, are to be submitted to the Tender inviting authority in a sealed envelope. Sealed envelope will contain the following: a) Hard copies of technical qualification related documents; b) A Pen drive containing soft copies of documents as mentioned in point (a) without any password; and c) Another Pen drive containing encrypted PDF file (password protected) of financial bid.

Bid Submission Checklist

S.No.	Format	Checklist (Yes/No)
1.	Cover Letter (on letterhead of the Bidder)	
2.	Declaration by Bidder for not being blacklisted	
3.	Integrity Pact	
4.	Non-Disclosure Agreement	
5.	Cloud Services Checklist	
6.	Commercial	

Declaration by Bidder for not being blacklisted

(To be submitted on the Letter head of the Bidder)

To,

**The Nodal Officer,
Independent Directors' Databank,
Indian Institute of Corporate Affairs,
Ministry of Corporate Affairs, Govt. of India
Plot No. 6, 7 & 8,
Sector 5, IMT Manesar,
Gurugram – 122052
Haryana**

Dear Sir,

We confirm that our Company <name of company> as on date of submission of the proposal is not blacklisted by any Private/Central /State Government/PSU or any other Organization and agencies in India or abroad for corrupt, fraudulent or any other unethical business practices.

Sincerely,

(Name & Designation of the Authorized Signatory)

Bid Evaluation method:

Evaluation will be based on the bidder meeting the Pre- qualification criteria and subsequent evaluation of financial

bid. It is mandatory for the bidder to fulfil all the Pre-qualification criteria to be technically qualified and for being considered for opening of their Financial Bid and evaluation thereof. The bidder with lowest financial quote (L1) shall be considered for award of contract.

A) Pre-Qualification

Bidder shall have to provide documentary evidence in support of the following mentioned Eligibility Criteria. In the absence of such supporting documents as mentioned against each criterion, the bid will be rejected summarily.

S. No.	Pre- Qualification Criteria (Technical)	Documents to be submitted by bidder
1.	Registration under Companies Act, 1956 and/or 2013 or LLP Act, 2008 Consortium of companies/ firms is not allowed.	1. Copy of Certificate of Incorporation or Certified copy of Partnership Deed.
2.	Empanelment with Meity under "Government Community Cloud Service Offerings" category.	Reference on Meity website or Empanelment Certificate
3.	The bidder should have valid GST registration and PAN number.	1. Copy of GST Registration Certificate 2. Copy of PAN
4.	The bidder should not be blacklisted by any Central Government/ State Government/ PSU/ Government Bodies/ Autonomous Bodies/ Private Sector or court of law.	The bidder shall furnish an undertaking duly attested by notary in a non-judicial stamp paper of value INR 100/-
5.	The bidder should be ISO 9001:2015, ISO 27001, or latest, certified as on date of submission of bid. The CSP of which bidder is an authorized partner should be ISO 27017 & ISO 27018 & ISO 22301 & PCI DSS Level1 or latest certified as on date of submission of bid.	Copy of the valid ISO Certificate issued from the accreditation organization.
6.	The bidder should have SOC1, SOC2 and SOC3 accreditations which are relevant to security, availability, processing integrity, confidentiality or privacy.	Copy of the valid certificates issued from the accreditation organization
7.	The DC & DR sites should be separated by a minimum distance of 100 kilometres.	Relevant documents to be submitted by the bidder duly signed and stamped.
8.	The bidder should have provided Cloud services at the bidder's Data centre in India for a minimum period of three completed years as on the date of submission of the bid i.e. in the year 21-22, 22-23, 23-24	Self-attested LOA/Work order and completion certificate to be submitted along with the bid.
9.	The bidder should have carried out at least 3 assignments in the aforesaid duration of a minimum work value of Rs.1 Cr each for the similar scope of work.	Work Order along with confirmation from client/Satisfactory Certificate.
10.	The Authorized Signatory signing the Bid on behalf of the bidder - should have the Power of Attorney duly authorized by the Board of Directors to sign the Bid.	Board Resolution or Power of Attorney on Non-Judicial stamp paper

1. Notwithstanding anything stated above, the IICA reserves the right to assess bidder's capability and capacity to perform the contract, should circumstances warrant such an assessment in the overall interest of the IICA or project.

2. IICA reserves the right to physically verify the office, or any document provided by the bidder in the way IICA desires.

B) Evaluation of Financial Bids

1. The Financial bid shall be opened for only those bidders who have been found to be technically qualified. The financial bids shall be opened in presence of representatives of technically qualified bidders, who may like to be present. IICA shall inform the date, place and time for opening of financial bids.

2. If there is any discrepancy between words and figures in any part of the financial bid, the amount indicated in words will prevail.

3. Financial bid should be checked by bidders to ensure conformance to the format provided in the tender

document.

4. The Bidder with lowest qualifying financial bid (L1) will be awarded AOC.

Integrity Pact

(To be executed on Stamp Paper of Hundred (INR 100.00) Rupees Stamp Paper)

This Agreement (hereinafter called the Integrity Pact) is entered into on ----day of the ----- month of 20-- -- between Indian Institute of Corporate Affairs, Ministry of Corporate Affairs, Govt. of India, acting through Shri -----(Name and Designation of the officer) (hereinafter referred to as the "IICA" which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and M/s. -----(Name of the company) represented by Shri -----, Chief Executive Officer / Authorized signatory (Name and Designation of the officer) (hereinafter called as the "Bidder / Seller / CSP" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS THE IICA invites bid for the

----- (Name of the Stores / Equipment / Service, Tender No. & Date) and the Bidder / Seller /CSP is willing to submit bid for the same and

WHEREAS the BIDDER is a private Company / Public Company / Government Undertaking / Partnership Firm / Ownership Firm / Registered Export Agency, constituted in accordance with the relevant law in the matter and

The IICA, NOW, THEREFORE

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence / prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to: -

- i. Enabling the IICA to obtain the desired said stores / equipment/ services/ works at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and
- ii. Enabling BIDDERS to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and IICA will commit to prevent corruption, in any form, by its officials by following transparent procedures. In order to achieve these goals, IICA will appoint an external independent monitor who will monitor the tender process and execution of the contract for compliance with the principles mentioned above.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows: -

1. COMMITMENTS OF IICA

IICA commits to take all measures necessary to prevent corruption and follow the system, that is fair, transparent and free from any influence / prejudice prior to, during and subsequent to the currency of the contract to be entered into to obtain stores / equipment / services at a competitive prices in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement.

The IICA undertakes that no employee of the IICA, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favor or any material or immaterial benefit or any other advantage from the Bidder, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

IICA will during the tender process treats all bidders with equity and reason. The IICA before and during the tender process provides to all bidders with the same information and will not provide any bidder any confidential information through which the bidder could obtain an advantage in relation to the tender process or execution of contract.

In case any such preceding misconduct on the part of such official(s) is reported by the Bidder to the IICA with full and verifiable facts and the same is prima-facie found to be correct by the IICA, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the IICA and such a person shall be debarred from further dealings related to the contract process. In such a case, while an enquiry is being conducted by the IICA, the proceedings under the contract will not be stalled.

2. COMMITMENTS OF THE BIDDERS / CONTRACTORS / SELLER / CSP

The Bidder commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it.

The Bidders will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the IICA, connected directly or indirectly with the bidding process or to any IICA person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

The Bidder further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the IICA or otherwise in procuring the contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with IICA for showing or forbearing to show favor or disfavor to any person in relation to the contract or any other contract with IICA.

The Bidders / Contractors will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal, in particular regarding prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

The Bidders/ Contractors will not commit any offence under relevant Anti-corruption Laws of India. Further, the Bidders will not use improperly, for purposes of competition or personal gain or pass on to others, any information or document provided by IICA as part of the business relationship regarding Plan, technical proposals and business details including information obtained or transmitted electronically.

The Bidders / Contractors of foreign origin shall disclose the names and addresses of agents / representatives in India, if any, and Indian Bidders shall disclose their foreign principals or associates.

The Bidder shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the IICA or any agency/ organization/consultant working with IICA.

The Bidder will not bring any Political, Governmental or Diplomatic influence to gain undue advantage in its dealing with IICA

The Bidder will promptly inform the Independent External Monitor (of IICA) if he receives demand for a bribe or illegal payment / benefit and If he comes to know of any unethical or illegal practice in IICA

The Bidders / Contractors will disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract while presenting his bid.

The Bidders / Contractors shall not lend or borrow any money from entering into any monetary dealings directly or indirectly, with any employee of the IICA or his relatives.

The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3. PREVIOUS TRANSGRESSION

The Bidder declares that no previous transgressions occurred in the last 3 years immediately before signing of this Integrity Pact, with any Government Organization (PSU / Municipalities/ Central or State Government Departments) in India in respect of any corrupt practices envisaged hereunder that could justify Bidder 's exclusion from the tender process.

If the Bidder makes an incorrect statement on this subject, he can be disqualified from the tender process or the contract if already awarded, can be terminated for such reasons.

4. DISQUALIFICATION FROM TENDER PROCESS AND EXCLUSION FROM FUTURE CONTRACTS

If the Bidders/ Contractors or anyone employee acting on his behalf whether or without the knowledge of the Bidder before award of the contract has committed a transgression through a violation of aforesaid provision or in any other form such as put his reliability or credibility into question, the IICA is entitled to exclude the bidder from the tender process or to terminate the contract if already signed and take all or any one of the following actions, wherever required.

To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the Bidder. Further, the proceedings with the other Bidders would continue.

The Performance Bond (after the contract is signed) shall stand forfeited either fully or partially, as decided by the IICA and IICA shall not be required to assign any reasons, therefore.

To immediately cancel the contract, if already signed, without giving any compensation to the

Bidder.

To recover all sums already paid with interest thereon at 5% higher than the prevailing Base rate of State Bank of India.

If any outstanding payment is due to the Bidder from IICA in connection with any other contract, such outstanding payment could also be utilized to recover the aforesaid sum and interest.

To encash any advance Bank Guarantee and performance bond/warranty, if furnished by the Bidder, in order to recover the payment already made by IICA along with interest.

To cancel all other contracts with the Bidder. The Bidder shall be liable to pay compensation for any loss or damages to the IICA resulting from such cancellation / rescission and the IICA shall be entitled to deduct the amount so payable from the money due to the Bidder.

Forfeiture of Performance Bond in case of a decision by the IICA to forfeit the same without assigning any reason for imposing sanction for violation of the Pact.

The decision of IICA to the effect that the breach of the provisions of this Pact has been committed by the Bidder shall be final and conclusive on the Bidder.

The Bidder accepts and undertakes to respect and uphold the absolute right of IICA to resort to and imposes such exclusion and further accepts and undertakes not to challenge or question such exclusion on any ground including the lack of any hearing before the decision to resort to such exclusion is taken.

To debar the Bidders/ Contractors from participating in future bidding process of IICA for a minimum period of one year for similar scope of services.

Any other action as decided by IICA based on the recommendation by Independent External Monitors (IEMs), if appointed for the bidding process.

5. VALIDITY OF THE PACT

The validity of this Integrity Pact shall be from the date of its signing and extend up to two years or the complete execution of the contract to the satisfaction of the IICA and BIDDER / Seller, including warranty period, whichever is later. In case BIDDER is unsuccessful, this Integrity Pact shall expire six months after the date of the signing of the contract.

If any claim is made/ lodged during the validity of this contract, such claim shall be binding and continue to be valid despite the lapse of this pact unless it is discharged / determined by the IICA.

6. FACILITATION OF INVESTIGATION

In case of any allegation of violation of any provisions of this Pact or payment of commission, the IICA or its agencies OR Independent External Monitor shall be entitled to examine all the documents including the Books of Accounts of the Bidder and the Bidder shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

7. MISCELLANEOUS

This Agreement / Pact is subject to the Indian Laws, place of performance and jurisdiction is the registered office of the IICA i.e. Indian Institute of Corporate Affairs, Sector 5, IMT, Manesar, Gurugram and the actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

If the Bidder is a partnership, this Agreement must be signed by all partners.

Should one or several provisions of this Agreement turn out to be invalid; the remainder of this Pact remains valid. In this case, the Parties will strive to come to an Agreement to their original intentions.

8. The Parties hereby sign this Integrity Pact at -----on-----

	IICA	BIDDER
Signature	-----	-----
Name of officer	-----	-----
Designation	-----	-----
Address	----- -----	----- -----
Dated	-----	-----
	WITNESS-1(IICA)	Witness-1(BIDDER)
Signature	-----	-----
Name of officer	-----	-----
Designation	-----	-----
Address	----- -----	----- -----
Dated	-----	-----

Non-Disclosure Agreement

(To be executed on Stamp Paper of Hundred (INR 100.00) Rupees Stamp Paper)

This Non-Disclosure Agreement ("Non-Disc") is made and entered into _____ day of _____ month _____ year (effective date) by and between IICA ("Department") and _____ ("Company")

Whereas, Department and Company have entered into an Agreement ("Agreement") effective _____ for _____; AND

Whereas each party desires to disclose to the other party certain information in oral or written form, which is proprietary and confidential to the disclosing party, ("CONFIDENTIAL INFORMATION").

NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein, the parties agree as follows:

1. Definitions. As used herein:

- a. The term "Confidential Information" shall include, without limitation, all information and materials, furnished by either Party to the other in connection with citizen/users/persons/customers data, products and/or services, including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic or optical media, and including all proprietary information, customer & prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, commercial or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to the disclosing party's data, computer database, products and/or services. Results of any tests, sample surveys, analytics, data mining exercises or usages, etc. carried out by the receiving party in connection with the Department's Information including citizen/users/persons/customers personal or sensitive personal information as defined under any law for the time being in force shall also be considered Confidential Information.
- b. The term, "Department" shall include the officers, employees, agents, consultants, contractors and representatives of Department.
- c. The term, "Company" shall include the directors, officers, employees, agents, consultants, contractors and representatives of Company, including its applicable affiliates and subsidiary companies.

2. Protection of Confidential Information. With respect to any Confidential Information disclosed to it or to which it has access, the Company affirms that it shall:

- a. Use the Confidential Information as necessary only in connection with the Project and in accordance with the terms and conditions contained herein.
- b. Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential
- c. Information that the parties take to protect the confidentiality of their own proprietary and confidential information and that of its clients.

- d. Not to make or retain copy of any commercial or marketing plans, citizen/users/persons/customers database, Proposals developed by or originating from Department or any of the prospective clients of Department except as necessary, under prior written intimation from Department, in connection with the Project, and ensure that any such copy is immediately returned to Department even without express demand from Department to do so;
 - e. Not disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the express written consent of the other party; and
 - f. Return to the other party, or destroy, at Department's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately upon the earlier to occur of (i) expiration or termination of either party's engagement in the Project, or (ii) the request of the other party therefore.
 - g. Not to discuss with any member of the public, media, press, any or any other person about the nature of arrangement entered between Department and Company or the nature of services to be provided by the Company to the Department.
3. **Onus** - Company shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the following exceptions.
4. **Exceptions** - These restrictions as enumerated in this Agreement shall not apply to any Confidential Information:
- a. Which is independently developed by Company or lawfully received from another source free of restriction and without breach of this Agreement; or
 - b. After it has become available to the public without breach of this Agreement by Company; or
 - c. Which at the time of disclosure to Company was known to such party free of restriction and evidenced by documentation in such party's possession; or
 - d. Which Department agrees in writing is free of such restrictions.
 - e. Which is received from a third party not subject to the obligation of confidentiality with respect to such Information.
5. **Remedies** - Company acknowledges that (a) any actual or threatened disclosure or use of the Confidential Information by Company would be a breach of this agreement and may cause immediate and irreparable harm to Department; (b) Company affirms that damages from such disclosure or use by it may be impossible to measure accurately; and (c) injury sustained by Department may be impossible to calculate and remedy fully. Therefore, Company acknowledges that in the event of such a breach, Department shall be entitled to specific performance by Company of Company's obligations contained in this Agreement. In addition, Company shall indemnify Department of the actual and liquidated damages which may be demanded by Department. Moreover, Department shall be entitled to recover all costs (including reasonable attorneys' fees) which it or they may incur in connection with defending its interests and enforcement of legal rights arising due to a breach of this agreement by Company.
6. **Need to Know**. Company shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know (and advise such employees of the obligations assumed herein), shall use the Confidential Information only for the purposes set forth in the Agreement, and shall not disclose such

Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of the disclosing party.

7. **Intellectual Property Rights Protection** - No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.
8. **No Conflict** - The parties represent and warrant that the performance of their obligations hereunder do not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.
9. **Authority** - The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.
10. **Dispute Resolution** - If any difference or dispute arises between the Department and the Company in connection with the validity, interpretation, implementation or alleged breach of any provision of this Agreement, any such dispute shall be referred to IICA, IICA
 - a. The arbitration proceedings shall be conducted in accordance with the (Indian) Arbitration & Conciliation Act, 1996 & amendments thereof.
 - b. The place of arbitration shall be New Delhi
 - c. The arbitrator's award shall be substantiated in writing and binding on the parties.
 - d. The proceedings of arbitration shall be conducted in English language.
 - e. The arbitration proceedings shall be completed within a period of 180 days from the date of reference of the dispute to arbitration.
11. **Governing Law** - This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to the exclusive jurisdiction of Courts and/or Forums situated at New Delhi, India only.
12. **Entire Agreement.** This Agreement constitutes the entire understanding and agreement of the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and understandings among the parties with respect to the subject matter hereof.
13. **Amendments** - No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.
14. **Binding Agreement** - This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.
15. **Severability** - It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.
16. **Waiver** - If either party should waive any breach of any provision of this Agreement, it shall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.
17. **Survival** - Both parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement shall survive till perpetuity even after any expiration or termination of this Agreement.

18. **Non-solicitation** - During the term of this Agreement and thereafter for a further period of two (2) years Company shall not solicit or attempt to solicit Department's employees and/or consultants, for the purpose of hiring/contract or to proceed to conduct operations/business similar to Department with any employee and/or consultant of the Department who has knowledge of the Confidential Information, without the prior written consent of Department. This section will survive irrespective of the fact whether there exists a commercial relationship between Company and Department.
19. This Agreement shall remain valid up to 1 year from the date of completion of Operational and Functional testing or up to such date and time as may be decided by IICA.

IN WITNESS HEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.

For Department,

For Company

Name:

Name:

Title:

Title:

WITNESSES:

- 1.
- 2.

Cloud Services Checklist

Sl. No.	Description of Cloud Service	Whether empanelled with Meity, with full compliance (Yes/No)
1.	Infrastructure as a Service (IaaS)	
2.	Platform as a Service (PaaS)	
3.	Disaster Recovery as a Service (DRaaS), with the DR site located in a different seismic zone.	
4.	Dev/Test Environment as a Service	
5.	Managed services: Backup services	
6.	Managed services: Disaster Recovery and Business Continuity Services	

Commercial Format / Financial Bid Proforma

- i. The Bidder has to quote the rate for the indicative Bill of Quantity provided in the Commercial sheet.
- ii. The bidder must share per unit pricing for each of the components listed in the Commercial sheet. The rates quoted are to be specified in “Per-Item-Per Hour” basis.
- iii. The cost quoted shall remain uniform for the entire duration of the contract (even the extension period of maximum 2 years on a yearly basis) and shall also remain uniform when scaling up and scaling down of the requirements.
- iv. Other Commercial indicators
 - a. All the prices are to be entered in Indian Rupees ONLY
 - b. The quantities mentioned are indicative in number.
 - c. The above charges must include DR provisioning with 100% computing as DC.
 - d. The Bidder needs to account for all Out of Pocket expenses due to Boarding, Lodging and other related items.
 - e. Prices indicated in the schedules shall be exclusive of all taxes, Levies, duties etc. During the payment period, IICA reserves the right to ask Bidder to submit proof of payment against any of the taxes, duties, and levies indicated.

Summary of Costs

Summary of Costs		
#	Items	Indicative cost per year (INR)
1.	IaaS	
2.	Bandwidth	
3.	Storage	
4.	Software Licenses	
5.	Gateways	
Total cost per year		

Item Heading	Description	Qty.	Remarks	Unit Rates		Extended Price				
				OTC Unit	Monthly Recurring Cost (Excluding GST)	OTC Total	Monthly Recurring Cost (Excluding GST) Year 1	Monthly Recurring Cost (Excluding GST) Year 2	Monthly Recurring Cost (Excluding GST) Year 3	
Internet bandwidth	Internet Bandwidth with Dedicated Router	10								
Firewall	Dedicated Firewall with IPS	1	with minimum 2.2 Gbps IPS throughput							
Production										

Cloud VMs	Linux-VirtualMachinewith4 Virtual CPU, 32GB Virtual RAM, 100 GB Virtual HDD on SAS disks inside VM, CloudOS-CentOS,1IPv4IP Address	1	Portal Server Apache Tomcat						
Cloud VMs	Linux-VirtualMachinewith8Virtual CPU,24GBVirtual RAM,500GB SSD (1500 IOPS) HDD on SAS disks inside VM, CloudOS-CentOS,1IPv4IPAddress	1	My SQL DB Master Slave						
Staging									
Cloud VMs	Linux-VirtualMachinewith4 Virtual CPU, 16 GB Virtual RAM, 100 GB Virtual HDD on SAS disks inside VM, CloudOS-CentOS,1IPv4IP Address	1	Portal Server Apache Tomcat						
Cloud VMs	Linux-VirtualMachinewith8Virtual CPU,24GBVirtual RAM,500GB SSD (1500 IOPS) HDD on SAS disks inside VM, CloudOS-CentOS,1IPv4IPAddress	1	My SQL DB Master Slave						
Storage	Storage Capacity (GB) with IOPS	500							
Backup Service	Backup services (GB)	1000							
Domain	Domain registration - Public Domain	1							
SSL Certificate	Digital Certificate-Thawte SSL 123 -1 year	1							
Security Services	HIPS	15	Secure Host Protection service works together to deliver Comprehensive security						
Security Services	SIEM (100EPS)	1							
Security Services	VA for Full Setup (Quarterly)	4							
Security Services	PT for web applications (Half yearly)	2							
Security Services	Audit (Quarterly)	4							
Security Services	DDOS (500Mbps)	1							
Infra Managed services	Managed Firewall	1	24*7Support						

Infra Managed services	Managed Operating system	4	24*7Support						
Infra Managed services	Managed database MySQL	2	24*7Support						
Infra Managed services	Managed SIEM	1	24*7Support						
Infra Managed services	Managed VA&PT	1	24*7Support						-
Mail Server	Dedicated	1							
			Total cost per Year (excluding GST)		Total	-	-	-	-
			Total cost per Year (including GST)		Total	-	-	-	-

Add-On Cloud Services

Bidder needs to provide the following costs. These will not be used as part of the commercial evaluation.

#	Add On Cloud Service	Hourly Rate (in INR)	Monthly Rate for VPC (INR)
1.	Per vCPU		
2.	Per GB RAM		
3.	Per50GB Storage		
4.	HSM Cost per instance		

*Inclusions but not limited to:

1. Managed VM
2. Operating System (Linux& Windows)
3. VLAN
4. Firewall
5. Bandwidth
6. Antivirus
7. Infrastructure Managed Services
8. Network Managed Services
9. Security Managed Services
10. Hardware Load Balancing
11. Admin Account
12. Backup
13. Bulk Mailing (cPanel)

6. Draft Contract Agreement

Definitions, Interpretations and Other Terms

- **Bid** means the tender process conducted by IICA and the technical and commercial proposals submitted by the successful bidder, along with the subsequent clarifications and undertakings, if any.
- **Confidential Information** means all information including IICA Data (whether in written, oral, electronic or other format) which relates to the technical, financial, business affairs, customers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party in the course of or in connection with this agreement (including without limitation such information received during negotiations, location visits and meetings in connection with this agreement);
- **Customers** mean all citizens and business organizations and users who use the IICA services.
- **Deliverables** means all the activities related to the Cloud and other service provisioning, as defined in the Bid Document & subsequent Corrigendum (if any), based on which the technical proposal & commercial proposal was submitted by the Bidder and as required as per this agreement.
- **Effective Date** means the date on which the Work Order or Letter of Acceptance is issued.
- This Agreement, together with the recitals, all schedules, and the contents, requirements, specifications and standards of the Bid Document (as may be amended, supplemented or modified in accordance with the provisions hereof) and the Bid. **In the event of a conflict between this agreement and the Schedules, the terms of the agreement shall prevail; with overriding effect.**
- **Performance Security** means the irrevocable and unconditional Bank Guarantee provided by the Service provider from any Nationalized/Scheduled bank in favor of Head, Centre for e-Governance, IICA for an amount equivalent to 10% of the total contract value.
- **Proprietary Information** means processes, methodologies and technical and business information, including drawings, designs, formulae, flow charts, data and computer programs already owned/licensed by either Party or granted by third parties to a Party hereto prior/ subsequent to the execution of this contract.
- **Required Consents** means the written consents, clearances and licenses, rights and other authorizations as may be required to be obtained by the Service Provider, for all tasks/activities/software/hardware and communication technology for this project; from all the concerned departments/agencies, etc. as the case may be.

- **Bid Document** means the Limited Tender Enquiry released vide Bid Document number [I-16012/2/2019-E-GOV](#) and include all clarifications/addendums, explanations and amendments issued by the department in respect thereof;
- **Services** means the content and services delivered and to be delivered to the customers or the offices of IICA by the Service Provider and includes but not limited to the services specified in the Bid Document or as may be specified and incorporated in the subsequent Agreement.
- **Users** mean the departmental staff or any other IICA officials having access to IICA Application Landscape including its Implementation Agencies, technology vendors, corporations and agencies and their employees, as the context admits or requires.

Interpretations

- References to any statute or statutory provision include a reference to that statute or statutory provision as from time to time amended, extended, re-enacted or consolidated and to all statutory instruments made pursuant to it.
- Words denoting the singular shall include the plural and vice versa and words denoting persons shall include firms and corporations and vice versa.
- Unless otherwise expressly stated, the words "herein", "hereof", "hereunder" and similar words refer to this agreement as a whole and not to any particular Article, Schedule. The term Articles refers to Articles of this agreement. The words "include" and "including" shall not be construed as terms of limitation. The words "day" and "month" mean "calendar day" and "calendar month" unless otherwise stated. The words "writing" and "written" mean "in documented form", whether electronic or hard copy, unless otherwise stated.
- The headings and use of the bold type in this agreement is for convenience only and shall not affect the interpretation of any provision of this agreement.
- The Schedules to this agreement form an integral part of this agreement and will be in full force and effect as though they were expressly set out in the body of this agreement.
- Reference at any time to any agreement, deed, instrument, license or document of any description shall be construed as reference to such agreement, deed, instrument, license or other document as the same may be amended, varied, supplemented, modified or suspended at the time of such reference.
- References to "construction" or "roll out" includes, unless the context otherwise requires, design, development, implementation, engineering, procurement, delivery, transportation, installation,

processing, fabrication, acceptance testing, certification, commissioning and other activities incidental to the construction or roll out, and “construct” or “roll out” shall be construed accordingly.

- Any word or expression used in this agreement shall, unless defined or construed in this agreement, bear its ordinary English language meaning.
- The damages payable by a Party to the other Party as set forth in this agreement, whether on per diem basis or otherwise, are mutually agreed genuine pre-estimated loss and liquidated damages likely to be suffered and incurred by the Party entitled to receive the same and are not by way of penalties.
- This agreement shall operate as a legally binding agreement specifying the master terms, which apply to the Parties under this agreement and to the provision of the services by the Service Provider.
- The department may nominate a technically competent agency/individual(s) for conducting acceptance testing and certification of the various requisite infrastructure to ensure smooth, trouble free and efficient functioning of the Scheme or carry out these tasks itself.
- The agency/individual nominated by the department can engage professional organizations to conduct specific tests on the software, hardware, networking, security and all other aspects.
- The agency/individual will establish appropriate processes for notifying the Service Provider of any deviations from the norms, standards or guidelines at the earliest instance after taking cognizance of the same to enable the Service Provider to take corrective action.
- Such involvement of and guidance by the agency/person will not, however, absolve the Service Provider of the fundamental responsibility of designing, installing, testing and commissioning the application & the infrastructure for efficient and effective delivery of services as contemplated under this Bid Document.
- The documents forming this Agreement are to be taken as mutually explanatory of one another. The following order shall govern the priority of documents constituting this Agreement, in the event of a conflict between various documents, the documents shall have priority in the following order:
 - This Agreement.
 - Scope of Services for the Bidder
 - Detail Commercial proposal of the Bidder accepted by IICA
 - Clarification & Corrigendum Documents published by IICA subsequent to the Bid Document for this work
 - Bid Document of IICA for this work

- LoI issued by IICA to the successful Bidder and
- Successful Bidder proposal submitted (including commercial proposal) in response to the Bid Document.

Term of the Contract Agreement

- The term of this agreement shall be for a period of one year. This excludes the days required for Bidder for implementation of Cloud services including migration and operational acceptance issued by IICA followed by one year maintenance and support which is extendable for two more years on a yearly basis.
- In the event of implementation period getting extended beyond the stipulated time, for reasons not attributable to the Bidder, IICA reserves the right to extend the term of the Agreement by corresponding period to allow validity of contract from the date of operational acceptance.

Work Completion Timelines & Payment Terms

#	Parameter	Timelines	Payment
1	Creation of cloud environment with required infrastructure and bandwidth	Within 7 days from issuance of work order	Nil
2	Migration of the application on the new Cloud environment	Within 9 days of issuance of work order	Nil
3	Operational Acceptance and Functional testing	Within 15 days of issuance of work order	Nil
4	Operation and Maintenance phase	For a period of one year	Quarterly Payment (QP) for a period of one year.

Disbursement of payment to the Bidder is based on completion of tasks indicated in the implementation plan.

Notes:

1. Adherence to timelines is critical for the success of the project.
2. No advance payment shall be made for any activity
3. If the Bidder is liable for any penalty as per the SLA (refer to the related clause of this agreement), the same shall be adjusted from payments due to the Bidder.
4. IICA will release the payment within 90 days of submission of a valid invoice subject to the condition that invoice and all supporting documents produced are in order and work is performed as per the scope of the project and meeting the SLA Criteria. IICA shall be entitled to delay or withhold the payment of a disputed invoice or part of it delivered by Bidder, when IICA disputes such invoice or part of it, provided that such dispute is Bonafide.
5. No payment made by IICA herein shall be deemed to constitute acceptance by IICA of the system

or any service

6. If the Bidder is liable for any penalty/liquidated damages as per the SLA, the same shall be adjusted from quarterly payments due to the service provider.
7. All payments shall be made for the corresponding to the services actually delivered.

Implementation related timelines and penalties

#	Parameter	Target	Basis	Penalty
1	Creation of cloud environment with required infrastructure and bandwidth	Within 7 days from issuance of work order	This will be calculated on basis of days of delay	a) Within 7 days - Nil b) Delay of 7 days 5% of QP. c) Delay of 14 days - 10% of QP d) Beyond 30 days - 50% of QP. The CSP would be required to provide proper justification for the delay. If IICA feels that the justification provided by the CSP is not credible, the contract may be terminated.

Note: In case where delay is beyond the scope and jurisdiction of the CSP the same shall be judged by IICA to assess the extent of penalty.

Service Level Agreements

1. The purpose of this Service Level Requirements/Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the Bidder to IICA for the duration of this contract period of the Project.
2. Timelines specified in the above section (Work Completion Timelines and Payment Terms) shall form the Service Levels for delivery of Services specified there-in.
3. All the payments to the Bidder are linked to the compliance with the SLA metrics specified in this document.

Commencement of SLA: The SLA shall commence from implementation period itself for adherence to the implementation plan. The penalty will be deducted from the next payment milestone during the implementation period. During the O & M period, the penalty will be deducted from the quarterly payments.

S. No	Parameter	Measurement Methodology	Basis	Penalty
1	Availability/Uptime of cloud services Resources for Production environment (VMs, Storage, OS, VLB, Security Components)	Availability (as per the definition in the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud.	Availability for each of the provisioned resources: >=99.5% measured on a monthly basis	<99.5% & >=99% (10% of the MP) < 99% (20% of the MP)
2	Availability of Critical Services (Register Support Request or Incident, Provisioning / De-Provisioning, Utilization Reports)	Availability will be measured for each of the critical services. VMs to be provisioned within 15 minutes if the utilization reaches 80%.	Availability for each of the critical services) >= 99.5% measured on a monthly basis	Default on any one or more of the services will attract penalty as indicated below. <99.5% and >= 99% (10% of the MP <99% (20% of the MP)

S. No	Parameter	Measurement Methodology	Basis	Penalty
3	Availability of the network links at DC, DR and Replication links	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud.	Availability for each of the network links: $\geq 99.5\%$ measured on a monthly basis	Default on any one or more of the provisioned network links will attract penalty as indicated below. $< 99.5\%$ & $\geq 99\%$ (10% of the MP) $< 99\%$ (30% of the MP)
4	Availability of SLA Reports		15 working days from the end of the quarter. Measured on a monthly basis	5% of MP
5	Adherence to RTO – Time to bring the infrastructure services till OS level available from the other site (DC/DR)	RTO is 2 Hours	Measured on a monthly basis	a) ≤ 2 Hours – Nil b) > 2 Hours to ≤ 3 Hours – 10% of MP c) > 3 Hours to ≤ 4 Hours – 15% of MP d) > 4 Hours to ≤ 5 Hours – 20% of MP
6	Adherence to RPO (Duration for which data is not available in case of any disaster at one site)	RPO is 30 minutes	Measured on a monthly basis	a) ≤ 30 min – Nil b) > 30 min to ≤ 45 min – 10% of MP c) > 45 min to ≤ 60 min – 15% of MP d) > 60 min to ≤ 75 min – 20% of MP

S. No	Parameter	Measurement Methodology	Basis	Penalty
7	Software Licenses	CSP is required to provide Enterprise level support or Equivalent for software licenses as mentioned in the LTE. Covering updates, security patches, issue resolution at software level, bug fixing etc.	Measured based on occurrence	<p>a) 24/7/365 days of unlimited support</p> <p>b) Response time – Within 45 min of logging the ticket</p> <p>i) Within 45 min – Nil</p> <p>ii) >45 to <=60 min – 10% of MP</p> <p>iii) >60 min to <=90 min – 15% of MP</p> <p>iv) >90 min – 20% of MP</p> <p>c) Issue Resolution time – Within 24 hours from the time of logging the ticket I)</p> <p><=24 Hours – Nil</p> <p>ii)>24 Hours to <=30 Hours – 10% of MP</p> <p>iii)>30 Hours to <=48 Hours – 15% of MP</p> <p>d)>48 Hours– 20% of MP</p>
8	Support Response time	Time taken to respond to Support calls	Measured based on severity	<p>a) 24/7/365 days of unlimited support</p> <p>b) 10% of the MP if Response time is more than as mentioned below</p> <ul style="list-style-type: none"> 15 min for business-critical calls

S. No	Parameter	Measurement Methodology	Basis	Penalty
				<p>(Application becomes unavailable)</p> <ul style="list-style-type: none"> • 6 hours for System Impaired Calls • 24 hours or less for general guidance calls
9	Security Incident	<p>If any security incident occurs and is proved to be caused through a vulnerability not addressed by CSP, the CSP shall be charged penalty per reported vulnerability (zero day vulnerability shall be excluded)</p>	<p>Measured based on occurrence</p>	<p>High risk vulnerability shall each attract a penalty of 10% of the MP</p> <p>Medium risk vulnerability shall each attract a penalty of 5% of the MP</p> <p>Note: The criteria for the criticality of security vulnerability shall be mutually discussed with IICA. If not agreed, standard practices shall be followed to define the criticality.</p>
10	Closure of security vulnerability	<p>Bidder shall perform regular security assessments (preferably every quarter) for the infrastructure managed by CSP and share the relevant report with IICA. Further, IICA may</p>	<p>Measured on a quarterly basis, or as and when security assessments are conducted</p>	<p>Delay in closure of High risk vulnerability shall each attract a penalty of 10% of the MP</p> <p>Delay in closure of Medium risk vulnerability shall each attract a penalty of 5% of the MP</p>

S. No	Parameter	Measurement Methodology	Basis	Penalty
		<p>also get security assessments conducted through external agencies. High risk security vulnerability shall be patched within 5 days of reporting vulnerability, whereas Medium risk security vulnerability shall be patched within 15 days of reporting.</p>		<p>Note: The criteria for the criticality of security vulnerability shall be mutually discussed with IICA. If not agreed, standard practices shall be followed to define the criticality.</p> <p>The delay will be considered if the delay is on account of the CSP.</p>
11	Incident Reporting (including security and other incidents)	<p>CSP shall update IICA on a monthly basis (within 7 days of next month) for the occurrence of any incidents. High criticality incidents shall be reported to IICA within 2 hours of occurrence / detection; Medium criticality incidents shall be reported to IICA within 8 hours of occurrence</p>	<p>Measured on a monthly basis, or as and when on occurrence</p>	<p>Delays in reporting of monthly incident report shall attract a penalty of 10% of the MP.</p> <p>Delay in reporting of High criticality incidents shall each attract a penalty of 10% of the MP</p> <p>Delay in reporting of Medium criticality incidents shall each attract a penalty of 5% of the MP</p> <p>Note: The criteria for the criticality of incidents shall be mutually discussed with IICA. If not agreed,</p>

S. No	Parameter	Measurement Methodology	Basis	Penalty
				<p>standard practices shall be followed to define criticality.</p> <p>The delay will be considered if the delay is on account of the CSP.</p>

***QP – Quarterly payment**

***MP – Monthly payment**

SLA's will be measured on Monthly basis and Payments for maintenance and support phase will be made on quarterly basis

Note:

1. The Bidder has to submit all the reports pertaining to the SLA Review process within 15 working days after the end of the quarter.
2. All the reports must be made available to IICA, as and when the report is generated or when asked by the competent authority.
3. In case the issue is still unresolved, the arbitration procedures described in the Terms & Conditions section will be applicable.
4. The down time will be calculated on a monthly basis. Non-adherence to any of the services as mentioned below will lead to penalty as per the SLA clause and will be used to calculate downtime. The downtime calculated shall not include the following
 - a. Down time due to the application which is owned by IICA at their premises
 - b. Failure or malfunction of any services not provided by the Bidder.
5. However, it is the responsibility of the selected Bidder to prove that the outage is attributable to IICA.
6. The total deduction per quarter shall not exceed 20% of the total QP value.
7. Two consecutive quarterly deductions amounting to more than 20% of the QPs on account of any reason will be deemed to be an event of default and termination

8. It is the right of the IICA to bring/deploy any external resources / agencies at any time for SLA review
9. No carrying forward of any penalties of SLA calculations can be done from any of the preceding quarters
10. The Agency shall deploy sufficient workforce suitably qualified and experienced in shifts to meet the SLA. Agency shall appoint as many team members as deemed fit by them, to meet the time Schedule and SLA requirements.

Professional Project Management

Bidder shall execute the project with complete professionalism and full commitment to the scope of work and the prescribed service levels. Bidder shall attend regular Project Review Meetings scheduled by IICA and shall adhere to the directions given during the meeting. The following responsibilities are to be executed by the Bidder in a regular manner to ensure the proper management of the project:

- a) Finalization of the Project plan in consultation with IICA and its consultants. Project Plan should consist of work plan, communication matrix, timelines, Quality Plan, IT Infrastructure Management Plan, etc.
- b) Preparation and regular update of the Risk Register and the Mitigation Plan. Timely communication of the same to all the identified project stakeholders
- c) Submission of Weekly Project Progress Reports
- d) Monthly Compliance report, which will cover compliances with Project Timelines, Hardware and Software, delivery, SLAs, etc.

Use & Acquisition of Assets during the term

The Bidder shall:

1. Take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components used for the project and other facilities leased/owned by the Bidder exclusively in terms of the delivery of the services as per this CA (hereinafter the "Assets") in proportion to their use and control of such Assets which will include all upgrades/enhancements and improvements to meet the needs of the project arising from time to time.
2. Term "Assets" also refers to all the hardware / Software / furniture / data / documentations / manuals/ or any other material procured, created or utilized by the Bidder or IICA for implementation of IT Infrastructure solution.
3. Keep all the tangible Assets in good and serviceable condition (reasonable wear and tear excepted) suitably upgraded subject to the relevant standards as stated in the bid to meet the SLAs mentioned in the contract and during the entire term of the Agreement.

4. Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of Assets and which are provided to the Bidder will be followed by the Bidder and any person who will be responsible for the use of the Asset
5. Take such steps as may be recommended by the manufacturer of the Assets and notify the Bidder or as may be necessary to use the Assets in a safe manner
6. To the extent that the Assets are under the control of the Bidder, keep the Assets suitably housed and in conformity with any statutory requirements from time to time applicable to them
7. Not, knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to law
8. Use the Assets exclusively for the purpose of providing the Services as defined in the contract
9. Ensure the integration of the software with hardware to be set up and the current Assets in order to ensure the smooth operations of the entire solution architecture to provide efficient services to IICA of this Project in an efficient and speedy manner
10. Bidder shall not use IICA data to provide services for the benefit of any third party, as a service bureau or in any other manner

Security and safety

1. The Bidder will comply with the directions issued from time to time by IICA and the standards related to the security and safety as far as it applies to the provision of the Services
2. Adherence to basic e-Governance Guidelines and Standards for data structure (if any) shall be adhered to.
3. Bidder shall also comply with IICA's information technology security and standard policies in force from time to time as applicable. IICA shall share the relevant guidelines and standards with the Bidder upon signing of the CA.
4. Bidder shall use reasonable endeavors to report forthwith in writing to all the partners / contractors about the civil and criminal liabilities accruing due to any unauthorized access (including unauthorized persons who are employees of any Party) or interference with IICA's data, facilities or Confidential Information.
5. The Bidder shall upon reasonable request by IICA or his/her nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.
6. Bidder shall promptly report in writing to IICA any act or omission which they are aware that could have an adverse effect on the proper conduct of safety and information technology security at IICA.

7. Bidder shall comply or meet any security requirements applicable to CSPs/Service Provider published (or to be published) by M/o E&IT or any standard body setup/recognized by Government of India from time to time and notified to the CSP/Service providers by M/o E&IT as a mandatory standard.
8. The Bidder shall meet all the security requirements indicated in the IT Act 2000 and Amendments 2008, international security standards including ISO 27001, the terms and conditions of the provisional Empanelment of the Cloud Service Providers and shall comply with the audit criteria defines by STQC. The bidder shall be responsible for the security of the infrastructure and services provided.

Performance Bank Guarantee

1. The Bidder shall at its own expense, deposit with department, within 3 days of the notification of award (done through issuance of the Purchase Order/Letter of Acceptance), an unconditional and irrevocable Performance Bank Guarantee (PBG) from Nationalized/Scheduled Bank as per the format included in this LTE, payable on demand, for the due performance and fulfillment of the contract by the Bidder. This Performance Bank Guarantee will be for an amount equivalent to 10% of contract value. All charges whatsoever such as premium, commission, etc. with respect to the PBG shall be borne by the Bidder.
2. The PBG would be valid for a period of 90 days more from the date of validity of the Contract. The PBG may be discharged/ returned by the department upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the PBG. In the event, Bidder being unable to service the contract for whatever reason, department would evoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of department under the Contract in the matter, the proceeds of the PBG shall be payable to department as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract. The department shall notify the Bidder in writing of the exercise of its right to receive such compensation within 14 days, indicating the contractual obligation(s) for which the Bidder is in default.
3. Department shall also be entitled to make recoveries from the Bidder's bills, PBG, or from any other amount due to him, the equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction or misstatement.

Indemnity

The Bidder agrees to indemnify and hold harmless IICA, its officers, employees and agents (each an "Indemnified Party") promptly upon demand at any time and from time to time, from and against any and all losses, claims, damages, liabilities, costs (including reasonable attorney's fees and disbursements) and expenses (collectively, "Losses") to which the Indemnified Party may become subject, in so far as such losses directly arise out of, in any way relate to, or result from

1. Any misstatement or any breach of any representation or warranty made by the Bidder or
2. The failure by the Bidder to fulfill any covenant or condition contained in this Agreement, including without limitation the breach of any terms and conditions of this Agreement by any employee or agent of the Bidder. Against all losses or damages arising from claims by third Parties that any Deliverable (or the access, use or other rights thereto), created by Bidder pursuant to this Agreement, or any equipment, software, information, methods of operation or other intellectual property created by Bidder pursuant to this Agreement, or the SLAs (I) infringes a copyright, trade mark, trade design enforceable in India, (II) infringes a patent issued in India, or (III) constitutes misappropriation or unlawful disclosure or use of another Party's trade secrets under the laws of India (collectively, "Infringement Claims"); provided, however, that this will not apply to any Deliverable (or the access, use or other rights thereto) created by "Implementation of the IT Infrastructure product by itself at the direction of IICA, or
 - a. Any compensation / claim or proceeding by any third party against IICA arising out of any act, deed or omission by the Bidder or
 - b. Claim filed by a worker or employee engaged by the Bidder for carrying out work related to this Agreement. For the avoidance of doubt, indemnification of Losses pursuant to this section shall be made in an amount or amounts sufficient to restore each of the Indemnified Party to the financial position it would have been in had the losses not occurred.

Any payment made under this Agreement to an indemnity or claim for breach of any provision of this Agreement shall include applicable taxes.

Third Party Claims

1. Subject to Sub-clause (b) below, the Bidder (the "Indemnified Party") from and against all losses, claims litigation and damages on account of bodily injury, death or damage to tangible personal property arising in favor of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's performance or non-performance under this Agreement or the SLAs.
2. The indemnities set out in Sub-clause (a) above shall be subject to the following conditions:

- a. The Indemnified Party, as promptly as practicable, informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise.
- b. The Indemnified Party shall, at the cost and expenses of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the defense of such claim including reasonable access to all relevant information, documentation and personnel. The indemnifying party shall bear the cost and expenses and fees of the Attorney on behalf of the Indemnified Party in the litigation, claim.
- c. If the Indemnifying Party does not assume full control over the defense of a claim as provided in this Article, the Indemnifying Party may participate in such defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be borne and paid by the Indemnifying Party.
- d. The Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party.
- e. Bidder hereby indemnifies and hold indemnified IICA harmless from and against any and all damages, losses, liabilities, expenses including legal fees and cost of litigation in connection with any action, claim, suit, proceedings as if result of claim made by the third party directly or indirectly arising out of or in connection with this agreement.
- f. All settlements of claims subject to indemnification under this Article will: (a) be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant for all liability in respect of such claim; and (b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement;
- g. The Indemnified Party shall take steps that the Indemnifying Party may require to mitigate or reduce its loss as a result of such a claim or proceedings; and
- h. In the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defenses of the Indemnified Party with respect to the claims to which such indemnification relates.
- i. In the event that the Indemnifying Party is obligated to indemnify the Indemnified Party pursuant to this Article, the Indemnified Party will be entitled to invoke the Performance Bank Guarantee (PBG), if such indemnity is not paid, either in full or in part, and on the invocation of the Performance Bank Guarantee, the Indemnifying Party shall be subrogated to all rights and

defenses of the Indemnified Party with respect to the claims to which such indemnification relates. The format for PBG is placed at Section 1.25.

3. Bidder will defend or settle third party claims against IICA solely attributable to the Bidder's infringement of any copyrights, trademarks or industrial design rights alleged to have occurred in respect of Bidder branded hardware/software/deliverables etc. (together "deliverables") supplied by the Bidder. The Bidder shall pay all costs, damages and attorney's fees that a court finally awards.
4. IICA shall provide the Bidder with prompt notice of such a claim and extend full cooperation and assistance, information and authority that is necessary to defend or settle such claim. The Bidder will have an adequate opportunity to control the response thereto and the defense thereof.
5. Further as an exclusion, the Bidder shall have no obligation for any claim of infringement to the extent arising from use of the deliverables in a way not indicated in the statement of work or in any specifications or documentation provided with such deliverable

Warranties

1. The Bidder warrants and represents to IICA that:
 - a. It has full capacity and authority and all necessary approvals to enter into and to perform its obligations under this Agreement.
 - b. This Agreement is executed by a duly authorized representative of the Bidder.
 - c. It shall discharge its obligations under this Agreement with due skill, care and diligence so as to comply with the service level agreement.
2. In the case of the SLAs, the Bidder warrants and represents to IICA, that:
 - a. The Bidder has full capacity and authority and all necessary approvals to enter into and perform its obligations under the SLAs and to provide the Services.
 - b. The SLAs shall be executed by a duly authorized representative of the Bidder.
 - c. The Services will be provided and rendered by appropriately qualified, trained and experienced personnel as mentioned in the bid.
 - d. Bidder has and will have all necessary licenses, approvals, consents of third Parties free from any encumbrances and all necessary technology, hardware and software to enable it to provide the Services.
 - e. The Services will be supplied in conformance with all laws, enactments, orders and regulations applicable from time to time.
 - f. Bidder will warrant that the solution provided under the contract is new, of the most recent higher version /models and incorporate all recent improvements in design and materials unless provided otherwise in the contract.

- g. Bidder shall ensure defect free operation of the entire solution and shall replace any such components, equipment, software and hardware which are found defective and during the entire contract period Bidder shall apply all the latest upgrades/patches/releases for the software after appropriate testing. No costs shall be paid separately for the warranty other than what the costs quoted by Bidder are as specified in the contract.
 - h. If the Bidder uses in the course of the provision of the Services, components, equipment, software and hardware manufactured by any third party and which are embedded in the Deliverables or are essential for the successful use of the Deliverables, it will pass through third party manufacturer's Warranties relating to those components, equipment, software and hardware to the extent possible.
3. Notwithstanding what has been stated elsewhere in this Agreement and the Schedules attached herein, in the event the Bidder is unable to meet the obligations pursuant to the Implementation of the IT Infrastructure Solution, Operations and Maintenance Services and any related scope of work as stated in this Agreement and the Schedules attached herein, IICA will have the option to invoke the Performance Guarantee after serving a written notice of thirty (30) days to the Bidder.

The 30 day notice period shall be considered as the 'Cure Period' to facilitate the Bidder to cure the breach. The PBG shall be evoked only if the breach is solely attributable to the bidder and the bidder fails to rectify the breach within the 'Cure Period.'

Force Majeure

The Bidder shall not be liable for forfeiture of its Performance Guarantee, imposition of liquidated damages or termination for default, if and to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. For purposes of this Clause, "Force Majeure" means an event beyond the "reasonable" control of the Bidder, not involving the Bidder's fault or negligence and not foreseeable. Unforeseen circumstances or causes beyond the control of the Bidder include but are not limited to acts of God, war, riot, acts of civil or military authorities, fire, floods, accidents, terrorist activity, strikes or shortages of transportation facilities, fuel, energy, labor or material.

For the Bidder to benefit of this clause it is a condition precedent that the Bidder must promptly notify IICA, in writing of such conditions and the cause thereof within five calendar days of the arising of the Force Majeure event. IICA, or the consultant / committee appointed by IICA shall study the submission of the Bidder and inform whether the situation can be qualified one of Force Majeure. Unless otherwise directed by IICA in writing, the Bidder shall continue to perform its obligations under the resultant Agreement as far as it is reasonably practical and shall seek all reasonable alternative means for performance of services not prevented by the existence of a Force Majeure event.

In the event of delay in performance attributable to the presence of a force majeure event, the time for performance shall be extended by a period(s) equivalent to the duration of such delay. If the duration of delay continues beyond a period of 30 days, IICA and the Bidder shall hold consultations with each other in an endeavor to find a solution to the problem.

Notwithstanding anything to the contrary mentioned above, the decision of IICA shall be final and binding on the Bidder.

Resolution of Disputes

IICA and the Bidder shall make every attempt to resolve dispute amicably, by direct information, negotiations of any disagreement or dispute arising between them under or in connection with this agreement. All disputes arising under and out of these present, or in connection with this agreement shall first be referred to by the senior executives of each party for an amicable solution. If the dispute is not resolved within a period of thirty (30) days, the same shall be referred to arbitration in accordance with the Arbitration and Conciliation Act, 1996 (including all amendments thereto). Each party shall appoint one arbitrator each and the two appointed arbitrators shall appoint the third arbitrator. The decision of the arbitrators shall be final and binding on both parties. The venue of arbitration shall be New Delhi, India. Subject to the above, this Agreement shall be subject to the jurisdiction of the courts in New Delhi, India.

Limitation of Liability towards IICA

The Bidder's liability under the resultant Agreement shall be determined as per the Law in force for the time being. The Bidder shall be liable to IICA for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the Bidder and its employees, including loss caused to IICA on account of defect in goods or deficiency in services on the part of Bidder or his agents or any person / persons claiming through or under said Bidder. However, such liability of Bidder shall not exceed the total value of the Agreement.

Bidder's aggregate liability in connection with obligations undertaken as a part of this contract regardless of the form or nature of the action giving rise to such liability, shall be at actuality and limited to the amount paid by IICA for:

- (i) The particular hardware/software; or
- (ii) Services provided during the twelve (12) months immediately preceding the date of the claim; that in each case is the subject of the claim.

This limit shall not apply to damages for bodily injury (including death) and damage to real property and tangible personal property for which the Bidder is legally liable.

Data Ownership

All the data created as part of the project shall be owned by IICA. The Bidder shall take utmost care in maintaining security, confidentiality and backup of this data. IICA shall retain ownership of any user created/loaded data and applications hosted on Bidder's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.

Fraud and Corruption

IICA requires that Bidder must observe the highest standards of ethics during the execution of the contract. In pursuance of this policy, IICA defines, for the purpose of this provision, the terms set forth as follows:

- "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of IICA in contract executions.
- "Fraudulent practice" means a misrepresentation of facts, in order to influence a procurement process or the execution of a contract, to IICA, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificially high or non-competitive levels and to deprive IICA of the benefits of free and open competition.
- "Undesirable practice" means (i) establishing contact with any person connected with or employed or engaged by IICA with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest; and
- "Restrictive practice" means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.
- "Coercive Practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract.
- If it is noticed that the Bidder has indulged into the Corrupt / Fraudulent / Undesirable / Coercive practices (as be decided by a court or competent authority with appropriate jurisdiction), it will be sufficient ground for IICA for termination of the contract and initiate black-listing of the vendor.

Conflict of Interest

- The Bidder shall disclose to IICA, in writing, all actual and potential conflicts of interest that exist arise or may arise (either for the Bidder or its team) in the course of performing the Services as soon as it becomes aware of such a conflict. Bidder shall hold IICA's interest paramount, without any consideration for future work, and strictly avoid conflict of interest with other assignments.

- In the event of any question, dispute or difference arising under the agreement or in connection therewith, the same shall be referred to the sole arbitration of the Chairman of Board, IICA or in case his designation is changed or his office is abolished, then in such cases to the sole arbitration of the officer for the time being entrusted (whether in addition to his own duties or otherwise) with the functions of the Chairman of Board, IICA or by whatever designation such an officer may be called (hereinafter referred to as the said officer), and if the Chairman of Board or the said officer is unable or unwilling to act as such, then to the sole arbitration of some other person appointed by the Chairman of Board or the said officer. The agreement to appoint an arbitrator will be in accordance with the Arbitration and Conciliation Act 1996. There will be no objection to any such appointment on the grounds that the arbitrator is a Government Servant or that he has to deal with the matter to which the agreement relates or that in the course of his duties as a Government Servant he has expressed his views on all or any of the matters in dispute. The award of the arbitrator shall be final and binding on both the parties to the agreement. In the event of such an arbitrator to whom the matter is originally referred, being transferred or vacating his office or being unable to act for any reason whatsoever, the Chairman of Board, IICA or the said officer shall appoint another person to act as an arbitrator in accordance with terms of the agreement and the person so appointed shall be entitled to proceed from the stage at which it was left out by his predecessors.
- The arbitrator may, from time to time with the consent of both the parties, enlarge the time frame for making and publishing the award. Subject to the aforesaid, arbitration and Conciliation Act, 1996 and the rules made there under, any modification thereof for the time being in force shall be deemed to apply to the arbitration proceeding under this clause.
- The venue of the arbitration proceeding shall be the office of the Chairperson of Board, IICA, or such other places as the arbitrator may decide.

Exit Management

(i) Exit Management Purpose

This clause sets out the provisions which will apply during Exit Management period. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Clause.

The exit management period starts, in case of expiry of contract, at least 3 months prior to the date when the contract ends or in case of termination of contract, on the date when the notice of termination is sent to the Bidder. The exit management period ends on the date agreed upon by IICA or Three months after the beginning of the exit management period, whichever is earlier.

(ii) Confidential Information, Security and Data

Bidder will promptly, at the commencement of the exit management period, supply to IICA or its nominated agencies the following:

- a. Information relating to the current services rendered and performance data relating to the performance of the services; documentation relating to the project, project's customized source code; any other data and confidential information created as part of or is related to this project.
- b. Project data as is required for purposes of the project or for transitioning of the services to replace successful Bidder in a readily available format.
- c. All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable IICA and its nominated agencies, or its replacing vendor to carry out due diligence in order to transition the provision of the Services to IICA or its nominated agencies, or its replacing vendor (as the case may be).
- d. The Bidder shall retain all of the above information with them for 30 days after the termination of the contract, post which the provider has to wipe/purge/delete all information created or retained as part of this project.
- e. Bidder will sign a Non-Disclosure Agreement with IICA IT Department. The format for the same has been included in Section 5.5.

(iii) Employees

Promptly on reasonable request at any time during the exit management period, the Bidder shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to IICA a list of all employees (with job titles and communication address) of the Successful Bidder, dedicated to providing the services at the commencement of the exit management period; To the extent that any Transfer Regulation does not apply to any employee of the Successful Bidder, IICA or Replacing Vendor may make an offer of contract for services to such employee of the Successful Bidder and the Successful Bidder shall not enforce or impose any contractual provision that would prevent any such employee from being hired by IICA or any Replacing Vendor.

(iv) Rights of Access to Information

At any time during the exit management period, the Bidder will be obliged to provide an access of information to IICA and / or any Replacing Vendor in order to make an inventory of the Assets (including hardware / Software / Active / passive), documentations, manuals, catalogs, archive data, Live data, policy documents or any other material related to implementation of IT Infrastructure Solution for IICA.

(v) Exit Management Plan

Successful Bidder shall provide IICA with a recommended "Exit Management Plan" within 90 days of signing the contract, which shall deal with at least the following aspects of exit management in relation to the SLA as a whole and in relation to the Project Implementation, the Operation and Management SLA and Scope of work definition.

- a) A detailed program of the transfer process that could be used in conjunction with a Replacement Vendor including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
- b) Plans for communication with such Successful Bidder, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on Project's operations as a result of undertaking the transfer.
- c) Plans for provision of contingent support to the implementation of IT Infrastructure Solution for a reasonable period (minimum one month) after transfer.
- d) Exit Management Plan shall be presented by the Bidder too and approved by IICA or its nominated agencies.
- e) The terms of payment as stated in the Terms of Payment Schedule include the costs of the Bidder complying with its obligations under this Schedule.
- f) During the exit management period, the Bidder shall use its best efforts to deliver the services.
- g) Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

Termination of contract

IICA may, without prejudice to any other remedy under this Contract and applicable law, reserves the right to terminate for breach of contract by providing a written notice of 30 days stating the reason for default to the Bidder and terminate the contract either in whole or in part:

- Where IICA is of the opinion that there has been such Event of Default on the part of the service provider which would make it proper and necessary to terminate this Contract and may include failure on the part of the service provider to respect any of its commitments with regard to any part of its obligations under its bid, the LTE or under this Contract
- Where it comes to IICA's attention that the service provider is in a position of actual conflict of interest with the interests of IICA, in relation to any of services arising out of services provided under the resultant contract or this LTE

- If the Bidder fails to deliver any or all of the project requirements / operationalization / Operational Acceptance of project within the time frame specified in the contract; or
- If the Bidder fails to perform any other obligation(s) under the contract.

Prior to providing a notice of termination to the Bidder, IICA shall provide the Bidder with a written notice of 30 days instructing the Bidder to cure any breach/ default of the Contract, if IICA is of the view that the breach may be rectified.

On failure of the Bidder to rectify such breach within 30 days, IICA may terminate the contract by providing a written notice of 30 days to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to IICA. In such an event the Bidder shall be liable for penalty imposed by IICA.

In the event of termination of this contract for any reason whatsoever, IICA is entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective continuity of the services which the Bidder shall be obliged to comply with and take all available steps to minimize the loss resulting from that termination/ breach, and further allow and provide all such assistance to IICA and/ or succeeding vendor, as may be required, to take over the obligations of the Bidder in relation to the execution/ continued execution of the requirements of this contract.

Confidentiality

- i. The service provider shall maintain the highest level of secrecy, confidentiality and privacy with regard thereto.
- ii. Additionally, the service provider shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities.
- iii. IICA shall retain all rights to prevent, stop and if required take the necessary punitive action against the service provider regarding any forbidden disclosure.
- iv. Service provider should provide non-disclosure agreement, which shall be duly approved by the IICA

For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

- a) Information is 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.

Miscellaneous

a) Confidentiality

"Confidential Information" means all information including Project Data (whether in written, oral, electronic or other format) which relates to the technical, financial and operational affairs, business rules, citizen information, design rights, know-how and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party (whether a Party to the contract or to the SLA) in the course of or in connection with the contract (including without limitation such information received during negotiations, location visits and meetings in connection with the contract or to the SLA) or pursuant to the contract to be signed subsequently.

Except with the prior written permission of IICA, the Bidder (including all partners) and its Personnel shall not disclose such confidential information to any person or entity not expected to know such information by default of being associated with the project, nor shall the Bidder and its Personnel make public the recommendations formulated in the course of, or as a result of the project. In matters pertaining to privacy of data, the Bidder (including all partners) shall not use any data for analytical/commercial reasons whatsoever.

The Bidder recognizes that during the term of this Agreement, sensitive data will be procured and made available to it, its Subcontractors and agents and others working for or under the Bidder. Disclosure or usage of the data by any such recipient may constitute a breach of law applicable causing harm not only to the Department whose data is used but also to its stakeholders. The function of IICA requires the Bidder to demonstrate utmost care, sensitivity and strict confidentiality. Any breach of this Article will result in IICA and its nominees receiving a right to seek injunctive relief and damage from the Bidder.

The restrictions of this Article shall not apply to confidential information that:

- a. Is or becomes available to the public through no breach of this Article by the Recipient; and
- b. Was in the recipient's possession free of any obligation of confidence prior to the time of receipt of it by the Recipient hereunder; and
- c. Is developed by the Recipient independently of any of discloser's Confidential Information; and

- d. Is rightfully obtained by the Recipient from third Parties authorized at that time to make such disclosure without restriction; and
- e. Is identified in writing by the Discloser as no longer proprietary or confidential; or
- f. Is required to be disclosed by law, regulation or Court Order, provided that the recipient gives prompt written notice to the Discloser of such legal and regulatory requirement to disclose so as to allow the Discloser reasonable opportunity to contest such disclosure.

To the extent that such disclosure is required for the purposes of this Agreement, either Party may disclose Confidential Information to:

- a. Its employees, agents and independent contractors and to any of its affiliates and their respective independent contractors or employees; and
- b. Its professional advisors and auditors, who require access for the purposes of this Agreement, whom the relevant Party has informed of its obligations under this Article and in respect of whom the relevant Party has informed of its obligations under this Article has used commercially reasonable efforts to ensure that they are contractually obliged to keep such Confidential Information confidential on terms substantially the same as set forth in this Article. Either Party may also disclose confidential Information or any entity with the other Party's prior written consent.

The provisions of this Article shall survive the expiration or any earlier termination of this Agreement.

b) Standards of Performance

The Bidder shall provide the services and carry out their obligations under the Contract with due diligence, efficiency and professionalism/ethics in accordance with accepted professional standards and practices. The Bidder shall always act with respect to any matter relating to this contract. The Bidder shall abide by all the applicable provisions / Acts / Rules / Regulations, Standing orders, etc. of Information Technology standard as prevalent in the country. The Bidder shall also conform to the standards laid down by or Government of India from time to time. Such standards and guidelines shall be shared with the Bidder by IICA up on signing of the Contract.

c) Care to be taken while working at IICA Office

Bidder should follow instructions issued by concerned Competent Authority from time to time for carrying out work at designated places. Bidder should ensure that there is no damage caused to any private or public property. In case such damage is caused, Bidder shall immediately bring it to the notice of concerned organization and IICA in writing and pay necessary charges towards fixing of the damage.

Bidder shall ensure that its employees/representatives don't breach privacy of any citizen or establishment during the course of execution or maintenance of the project.

d) Compliance with Labour regulations

The Bidder shall pay fair and reasonable wages to the workers employed, for the contract undertaken and comply with the provisions set forth under the Minimum wages Act and the Contract Labour Act 1970. The salary of the workforce working on the IICA project should be paid using ECS / NEFT / RTGS. A record of the payments made in this regard should be maintained by the Bidder. Upon request, this record shall be produced by the appropriate authority in IICA and/or Judicial Body. If complaints are received by IICA (or any appropriate authority) appropriate action (Liquidation of Security Deposit, Blacklisting, etc.) may be initiated as deemed necessary against the Bidder.

e) Independent Contractor

Nothing in this Agreement shall be construed as establishing or implying any partnership or joint venture or employment relationship between the Parties to this Agreement. Except as expressly stated in this Agreement nothing in this Agreement shall be deemed to constitute any Party as the agent of any other Party or authorizes either Party (i) to incur any expenses on behalf of the other Party, (ii) to enter into any engagement or make any representation or warranty on behalf of the other Party, (iii) to pledge the credit of or otherwise bind or oblige the other Party, or (iv) to commit the other Party in any manner whatsoever in each case without obtaining the other Party's prior written consent.

f) Waiver

A waiver of any provision or breach of this Agreement must be in writing and signed by an authorized official of the Party executing the same. No such waiver shall be construed to affect or imply a subsequent waiver of the same provision or subsequent breach of this Agreement.

g) Notices

Any notice or other document, which may be given by either Party under this Agreement, shall be given in writing in person or by pre-paid recorded delivery post.

In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below:

**Nodal Officer,
Independent Directors' Databank
Indian Institute of Corporate Affairs
Ministry of Corporate Affairs, Govt. of
India Plot No. 6, 7 & 8, Sector 5, IMT,
Manesar Haryana, PIN – 122052**

Bidder:

Tel:

Fax:

Any notice or other document shall be deemed to have been given to the other Party when delivered (if delivered in person) if delivered between the hours of 9.30 am and 5.30 pm at the address of the other Party set forth above or on the next working day thereafter if delivered outside such hours, and 7 calendar days from the date of posting (if by letter).

h) Personnel/Employees

Personnel/employees assigned by Bidder to perform the services shall be employees of Bidder, and under no circumstances will such personnel be considered as employees of IICA. Bidder shall have the sole responsibility for supervision and control of its personnel and for payment of such personnel's employee's entire compensation, including salary, legal deductions withholding of income taxes and social security taxes, worker's compensation, employee and disability benefits and the like and shall be responsible for all employer obligations under all laws as applicable from time to time. IICA shall not be responsible for the above issues concerning the personnel of Bidder.

Bidder should use its best efforts to ensure that sufficient Bidder personnel are employed to perform the Services, and that such personnel have appropriate qualifications to perform the Services. IICA or its nominated agencies shall have the right to require the removal or replacement of any Bidder personnel performing work under this Agreement. In the event that IICA requests that any Bidder personnel be replaced, the substitution of such personnel shall be accomplished pursuant to a mutually agreed upon schedule and upon clearance of the personnel based on profile review and personal interview by IICA or its nominated agencies as per defined SLAs. The Bidder shall depute quality team for the project and as per requirements IICA shall have the right to ask Bidder to change the team.

- a. Management (Regional Head / VP level officer) of Bidder needs to be involved in the project monitoring and should attend the review meeting at least once in a month.
- b. The profiles of resources proposed by Bidder in the technical bid, which are considered for Technical bid evaluation, shall be construed as 'Key Personnel' and the Bidder shall not remove such personnel without the prior written consent of IICA. For any changes to the

proposed resources, Bidder shall provide equivalent or more experienced resources in consultation with IICA.

- c. Except as stated in this clause, nothing in this Agreement will limit the ability of Bidder freely to assign or reassign its employees; provided that Bidder shall be responsible, at its expense, for transferring all appropriate knowledge from personnel being replaced to their replacements. IICA shall have the right to review and approve Bidder's plan for any such knowledge transfer. Bidder shall maintain the same standards for skills and professionalism among replacement personnel as in personnel being replaced.
- d. Each Party shall be responsible for the performance of all its obligations under this Agreement and shall be liable for the acts and omissions of its employees and agents in connection therewith.

i) Variations & Further Assurance

- a. No amendment, variation or other change to this Agreement or the SLAs shall be valid unless made in writing & signed by the duly authorized representatives of the Parties to this Agreement.
- b. Each Party to this Agreement or the SLAs agree to enter into or execute, without limitation, whatever other agreement, document, consent & waiver & to do all other things which shall or may be required to complete & deliver the obligations set out in the Agreement or the SLAs.

j) Severability & Waiver

- a. if any provision of this Agreement or the SLAs, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the SLAs or the remainder of the provisions in question which shall remain in full force & effect. The relevant Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid or unenforceable provision, a valid & enforceable provision which achieves to the greatest extent possible the economic, legal & commercial objectives of the illegal, invalid or unenforceable provision or part provision within 7 working days.
- b. No failure to exercise or enforce & no delay in exercising or enforcing on the part of either Party to this Agreement or the SLAs of any right, remedy or provision of this Agreement or the SLAs shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of any other right, remedy or provision.

k) Survivability

The termination or expiry of this Agreement or the SLAs for any reason shall not affect or prejudice any terms of this Agreement, or the rights of the Parties under them which are either expressly or by implication intended to come into effect or continue in effect after such expiry or termination.

Applicable Law

The contract shall be governed by the laws and procedures prescribed by the Laws prevailing and in force in India, within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/processing. All legal disputes are subject to the jurisdiction of New Delhi courts only.

Attachments to the Agreement:

- i) Scope of Services for the bidder
- ii) Detail Commercial proposal of the Bidder accepted by IICA
- iii) Corrigendum Document published by IICA subsequent to the Bid Document for this work
- iv) Bid Document of IICA for this work
- v) Work Order issued by IICA to the successful bidder
- vi) The successful bidder's "Technical Proposal" and "Commercial Proposal" submitted in response to the Bid Document

Performance Bank Guarantee Format

(10% of Total Contract Value)

PERFORMANCE SECURITY:

Ref. No. :

Date :

Bank Guarantee No. :

To,

**Nodal officer,
Independent Directors' Databank
Indian Institute of Corporate Affairs
Ministry of Corporate Affairs, Govt. of India
Plot No. 6, 7 & 8, Sector 5, IMT, Manesar
Haryana, PIN – 122052**

Whereas <<name of the bidder and address>> (hereinafter called "Service Provider") has undertaken, in pursuance of Tender no. <Insert Tender No.> dated. <Date> to provide Cloud services for hosting AB-NHPM of IICA (hereinafter called "the beneficiary")

And whereas it has been stipulated by in the said contract that the bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract.

And whereas we, <Name of Bank> a banking company incorporated and having its head /registered office at <Address of Registered Office> and having one of its offices at <Address of Local Office> have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the supplier, up to a total of Rs.<Insert Value> (Rupees <Insert Value in Words> only) and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of Rs. <Insert Value> (Rupees <Insert Value in Words> only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you and the Service provider shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

This Guarantee shall be valid until <<Insert Date>>)

Notwithstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed Rs. <Insert Value> (Rupees <Insert Value in Words> only).

II. This bank guarantee shall be valid up to <Insert Expiry Date>)

III. It is the condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before <Insert Expiry Date>) failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

Seal:

Date:

7. Annexure 1: Data Security & Privacy Requirements

The Cloud Service Provider (CSP) shall be responsible for protecting the privacy, confidentiality, and security of the personal records/data of the registered users of the ID DB Portal. CSP shall setup framework to comply with international standards for portal user data protection including HIPAA, ISO 27001, and applicable regulations including IT Act and Amendments, Aadhaar Act and Regulations, and proposed data privacy Act and Regulations including Data Protection Act and Digital Information Security.

CSP shall develop information security and privacy framework including information security and privacy policy, procedures, and guidelines. CSP shall ensure that these security and privacy requirements are being adequately implemented across the infrastructure setup. The effectiveness shall be evaluated on a regular basis to ensure the continuity of security and privacy requirements.

The CSP shall ensure the security and privacy requirements including, but not limited to, the following:

- Design and develop information security and privacy framework in line with international standards including HIPAA, ISO 27001, and applicable regulations including IT Act and Amendments, Aadhaar Act and Regulations.
- Ensure the compliance with security requirements as detailed above and also to requirements and guidelines published by IICA from time to time. CSP shall also ensure compliance with upcoming security and privacy requirements as and when these become applicable.
- Set up an assurance process to periodically review the compliance with security and privacy requirements.
- Ensure that a secure network architecture comprising of appropriate security products is put in place to protect against different security risks.
- Only licensed software and hardware are used to provide services to IICA. CSP shall be responsible for the maintenance of all software managed with the latest updates, specifically related to security vulnerabilities.
- Ensure that the systems and devices are protected from viruses, malware, and any other security threats.
- Establish a patch management process to regularly update the systems and devices.
- Host the systems and devices processing the portal user data within the data centers located in India.
- Ensure policies & procedures for secure disposition of electronic data and hardware on which the data resides (e.g., wiping hard drive, or other methods of destruction)
- Ensure maintenance of system and application audit logs in line with applicable regulations including IT Act and Amendments, Aadhaar Act, and any other Regulations made applicable from time to time.

- Set up a robust incident / breach notification process to timely intimate appropriate stakeholders and respond to incidents / breach as per the Regulatory requirements, and international best practices.
- IICA shall have authority to conduct (or through external agency) periodical assessment of the security requirements to ensure compliance with security policies, procedures, and Regulations.
- CSP shall have an appropriate contingency plan (including backup) to recover the services / data as and when required (including during any disaster)

The service provider shall keep the confidentiality, maintain secrecy of all confidential information and shall not, at any time, divulge such or any part thereof to any third party except as may be compelled by any court or agency of competent jurisdiction, or as otherwise required by law, and shall also ensure that same is not disclosed to any person voluntarily, accidentally or by mistake.

1. **Compliance with Aadhaar Act and Regulations:** The Service Provider and all their associates shall comply with the relevant provisions of the Aadhaar Act 2016 and the Aadhaar Regulations 2016, while receiving, transmitting, storing, processing or handling Aadhaar Data, including Aadhaar Number, Demographic and Bio-metric data. Without prejudice to the specific provisions of the Act and the Regulations, the following provisions are brought to the notice of the bidders.
 - a. Any individual, entity or agency, which is in possession of Aadhaar number(s) of Aadhaar number holders, shall ensure security and confidentiality of the Aadhaar numbers and of any record or database containing the Aadhaar numbers.
 - b. Any individual, entity or agency, which is in possession of Aadhaar number(s) of Aadhaar number holders shall not make public any database or record containing the Aadhaar numbers of individuals, unless the Aadhaar numbers have been redacted or blacked out through appropriate means, both in print and electronic form.
 - c. Such individual, agency or entity shall not share the Aadhaar number with any person or entity.
 - d. No entity, including a requesting entity, shall require an individual to transmit his Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances.
 - e. No entity, including a requesting entity, shall retain Aadhaar numbers or any document or database containing Aadhaar numbers for longer than is necessary for the purpose specified to the Aadhaar number holder at the time of obtaining consent.
2. **Privacy of the Personal Records of Portal users:**
 - a. The provisions of the IT Act 2000 and any other Act / Rules / Regulations / Guidelines of Government of India shall be strictly followed while dealing with the Personal records of the users registered on the ID DB Portal.
 - b. The personal records of the users registered on the ID DB Portal shall not be shared with any individual or entity.
 - c. The personal records of the users registered on the ID DB Portal shall not be published on any website.

8. Annexure 2 - Strategic Control of Operations to be provisioned

While IICA has planned to outsource most of its IT operations as managed services, the final strategic control and governance shall still be with IICA for all its IT landscape management and operations. For ensuring strategic control of the operations –

1. The CSP shall provide self-service tools to IICA that can be used to manage their cloud infrastructure environments including Government Department specific configurations.
2. Approval of IICA shall be taken prior to making changes / modifications of the deployed solution, database, data, configurations, security solutions, hosted infrastructure, etc. of the Government Community Cloud where such changes may affect the solutions of IICA.
3. Where required, IICA shall be provided with the access rights on the cloud services console that will enable authorized IICA users to approve any critical changes to the solution including the underlying infrastructure before they are carried out by the CSP.
4. For any changes (including auto-provisioning and others that may or may not need prior approval) to the underlying cloud infrastructure, software, etc. under the scope of the CSP, that has the potential to affect the SLAs (performance, availability, etc.), IICA shall get alerts / notifications from the CSP, both as advance alerts and post implementation alerts.
5. The CSP shall provide access to IICA authorized users for the following roles -
 - Application Administration (including access to tools and logs)
 - Database Administration (including access to tools and logs)
 - Security Administration & Auditing (including access to tools and logs)
 - EMS & SLA monitoring tools and logs
 - Version Control Tools

For each role IICA will designate authorized officials. All approval requests for any change implementations as explained in points above need to be approved by both the designated officers. IICA at its discretion may involve further users to facilitate strategic control.