SCHOOL OF OPEN LEARNING
(CAMPUS OF OPEN LEARNING)
UNIVERSITY OF DELHI
5, CAVALRY LANE
DELHI-110007

TENDER DOCUMENT FOR SELECTION OF MANAGED SERVICE PROVIDER (MSP) FOR IMPLEMENTATION OF CLOUD SERVICES, SCHOOL OF OPEN LEARNING

CONTENTS OF TENDER DOCUMENT

e-TENDER NOTICE

Officer on Special Duty (OSD) , School of Open Learning, University of Delhi invites online tenders under Two Bids System (Technical and Financial) from eligible and reputed firms for selection of Managed Service Provider (MSP) for implementation of Cloud Services in School of Open Learning on the terms and conditions enumerated in detail in the tender document.

Item	Details / Date
EMD	Rs.60,000/-
Bid Submission Start Date	04/11/19 (03.00 P.M.)
Bid Submission End Date	15/11/19 (05:30 P.M.)
Bid Opening Date	18/11/19 (11:00 A.M.)

Notes:

(i) All details regarding the subject tender are available on our websites sol.du.ac.in and https://eprocure.gov.in/eprocure/app. Bidders are therefore, requested to visit our websites regularly to keep themselves updated.

(ii) Manual bids shall not be accepted.

(iii)For submission of E-Bids, bidders are required to get themselves registered with http://eprocure.gov.in/eprocure/app.

(iv) EMD should be in the form of Account Payee DD in favour of Officer on Special Duty (OSD) , SOL, University of Delhi, & should reach the Section Officer (General)**, Room No: 206, 2nd Floor, SOL, University of Delhi, Delhi-110007, on or** before the last date and time of bid submission, failing which offer will be liable for rejection. Bidders, however, have to upload scanned copy of EMD along with their other document.

(v) More information useful for submitting the online bids on CPP Portal may be obtained at: http://eprocure.gov.in/eprocure/app.

SECTION OFFICER (GENERAL)

SECTION-I

INTRODUCTION

1. INTRODUCTION

1.1 BACKGROUND

The School of Open Learning (SOL), formerly known as the School of Correspondence Courses and Continuing Education under the aegis of University of Delhi, is one of the pioneer institutions in the field of distance education in India. The School offers undergraduate/postgraduate degree courses in subjects of Humanity/Commerce in conventional mode.

1.2 BRIEF DESCRIPTION OF BIDDING PROCESS

a) SOL invites online bids under Two Bids System (Technical and Financial) from eligible and reputed firms for Selection of Managed Service Provider (MSP) for implementation of Cloud Services in School of Open Learning meeting eligibility criteria as specified in this document.

b) SOL will determine the bidders who meet the specified eligibility criterion for similar nature of work, to be called "Technically Qualified Bidders".

c) The Financial Bid of Technically Qualified Bidders only will be evaluated.

d) SOL will determine the lowest rates offered by "Technically Qualified Bidder".

e) The SOL will intimate the Technically Qualified Bidder for acceptance of the Approved Rates and the terms of contract.

f) Terms have been used interchangeably as under:
bidder includes tenderer;
bid includes tender;
bidding document includes tender document.

SECTION II

SCOPE OF WORK

2.1 Managed Service Provider (MSP) services for Cloud

As part of the managed services that will be required to be undertaken by the MSP, a broad categorization of the scope of work is given below

Serial No.	Activity
1	Provisioning and Setup of Cloud Services
2	Operations & Maintenance with optimization of Cloud services
3	Acceptance and Validation of Cloud Environment
4	Exit Management Plan/ Transition-Out Services and training.
5	Supply of required software licenses (as part of PaaS)
6	Manpower detailing

The details of the activities to be undertaken under each of the above category are as follows

2.2 Provisioning of Cloud Services – Infra, compute, storage, band-width

a) The MSP shall align a CSP of designated credentials.

b) The MSP shall be responsible for provisioning of required software, infrastructure, bandwidth, licenses and management of services deployment, including the underlying application/system software necessary to run the applications. It will be required to adequately and optimally size the necessary compute, memory, and storage required, build the minimum sufficient redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the Tender document at all times. The hosting solution must be designed for rapid elasticity and handle hardware failures without downtime. In addition to the production environment, the MSP shall also provision for the test and development environments (1 instance each respectively) on the cloud.

c) The MSP needs to carry out the capacity planning in advance, in consultation with SOL, to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution.

d) The Database nodes (RDBMS) should be in a separate subnet with higher security layer. The testing and development instances of the application should be in a separate subnet from the production instance and setup such that users of the environments are in separate networks.

2.3 Operations & Maintenance with optimization of Cloud services

The MSP would be required to undertake following activities as part of O&M of the cloud hosted applications:

a) While the minimum required compute and storage is provided in the Tender Document, it is expected that compute and storage requirements may be auto-scaled over the period of the contract in line with the transaction load and in order to meet the SLA requirements. The review of auto-scaling rules and limits may be done from time-to-time and approvals from SOL to be sought, wherever necessary. The MSP shall provide the necessary details like the sizing calculations, assumptions, current workloads & utilizations, expected growth / demand and any other details justifying the request to scale up or scale down
b) The MSP should ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity. Additionally, regular vulnerability scanning and penetration testing of the systems would be required, as per the best practices and in accordance with security policies of SOL. The audit logs will have to be reviewed to identify any unauthorized access to the systems and application.
c) Review of the service level reports provided by the CSP and monitoring of the service levels including availability, uptime, performance, and resource utilization of the network, storage, database, operating systems, all applications, including API access within the CSP's boundary would be diligently conducted by the MSP in order to identify any deviations from the SLAs and report SLA breaches to SOL. The MSP would monitor, manage and administer the billing related aspects that will help SOL to validate the billing of the CSP and SLA related penalties.
d) Configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases as per the backup policy of SOL. The MSP would assist restoration from the backup, as and when required.
e) Create and maintain all the necessary technical documentation, design documents, standard operating procedures, configurations required to continued operations and maintenance of cloud services.
f) Coordinate with the SOL team and the Data Centre team to manage business continuity and also provide reliable, secured and satisfactory cloud services to SOL for its Applications in cloud.
g) The payment shall be made against the invoices raised by the MSP in INR only (irrespective of the invoices raised by CSP in different currency) and the prices mentioned in the contract should only be valid for the entire contract period. Any increase in prices during the period of contract shall be to the Bidder's account. In case of reduction in the prices, SOL shall take the benefit of reduction in price from the date of reduction in prices. Any price increase at the end of year 1 will be notified separately to SOL.

2.4 Acceptance and Validation of Cloud Environment

a) Bidder shall validate after initial acceptance and within 6 months. The dates for demonstration will be mutually agreed.
b) Bidder has to factor the cost of provisioning the licenses, infrastructure, database instances, and any other services required to accept/validate the cloud environments.
c) Any licenses (OS, DB) required for such acceptance/validation is the responsibility of the bidder.

2.5 Exit Management Plan / Transition-Out Services

The MSP would be required to complete following activities: -

a) Exit Management plan shall be furnished in writing to the Purchaser or its nominated agencies at least 30 days before expiry of the contract.
b) Create the environment in client identified data centre and migrate all applications with data.
c) Retain the data at the end of the agreement (for a maximum of 30 days beyond the expiry of the Agreement). If data is to be retained the cost for retaining the data may be obtained in the commercial quote and SOL to pay for the same.
d) Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of the SOL.
e) Support and assist SOL for a period of 2 weeks to successfully deploy and access the services from the new environment.
f) Train and transfer the knowledge to the SOL to ensure similar continuity and performance of the Services post expiry of the Agreement.
g) The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with SOL.

2.6 Support of required software license and configuration

Bidder need to support on Installation and configuration of the licenses and deployment, as if required by Dept.

2.7 Cloud Services Specifications and Requirements

2.7.1 Regulatory Requirements

	Requirement	Description
1.	Data centre locations must be within India	Cloud provider should offer cloud services from within India and within the Indian I.P. address range
2.	Maintain and ensure data locality	Cloud provider should ensure that customer data resides only in the region they specify.
3.	Protect applications from the failure of a single location	Solution should be architected to run on cloud services offered from multiple data centre facilities to provide high availability with no interruptions in case of any disruptions to one of the data center facility. In case of failure, automated processes should move customer data traffic away from the affected area. The Cloud Service Provider should provide adequate bandwidth between the Data Centre Facilities to provide high availability. Region indicates India as a region. Application should be hosted from India Data Centers.

2.7.2 Compute

	Requirement	Description
1.	Compute instances – General Purpose Memory optimized Compute optimized Storage optimized GPU instances	Cloud provider should offer the following instance types – • General Purpose – optimized for generic applications and provides a balance of compute, memory, and network resources. • Memory optimized – optimized for memory applications • Compute optimized – optimized for compute applications • Storage optimized – include very fast/large amount of local storage for NoSQL databases and Hadoop
2.	Compute instances – Burstable performance	Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.
3.	Compute instances – Dedicated	Cloud provider should offer instances that run on hardware dedicated to a single customer.
4.	OS Support – Linux	Cloud provider should be able to support following Linux distributions - (Red Hat, SUSE, Ubuntu, CentOS)
5.	OS Support – Windows	Cloud provider should be able to support the last two major Windows Server versions (Windows Server 2016, Windows Server 2012)
6.	Resize virtual cores, memory, storage seamlessly	Customer must be able to specify and modify server configuration (CPU, memory, storage) parameters seamlessly for horizontal scaling without outage but can be allowed a maintenance window for vertical scale-up.
7.	Local disk/Instance store	Cloud service should support local storage for compute instances to be used for temporary storage of information that changes frequently.
8.	Provision multiple concurrent instances	Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.
9.	Instance affinity - logical grouping of instances within a single data centre	Customer should be able to logically group instances together for applications that require low network latency and/or high network throughput.

10.	Auto Scaling support	Cloud service should be able to automatically increase the number of instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
11.	Bring your own image/Instance Import	Customer should be able to import their existing image and save it as a new, privately available image that can then be used to provision instances in the future.
12.	Export Instance Image	Cloud service must support the ability to take an existing running instance or a copy of an instance and export the instance into a VMDK or VHD image format.
13.	Instance maintenance mitigation	Cloud service must be architected in such a way to avoid instance outages or downtime when the provider is performing any kind of hardware or service maintenance.
14.	Instance failure recovery	Cloud service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails.
15.	Instance restart flexibility	Cloud provider must be able to schedule events for customer's instances, such as a reboot, stop/start, or retirement. Depending on the event, customer might be able to take action to control the timing of the event.
16.	Support for Docker containers	Cloud service should support containers, including Docker and/or other containerization platforms.
17.	Highly scalable, high performance container management service	Cloud provider should offer a highly scalable, high performance container management service.
18.	Event-driven computing that runs code in response to events	Our requirement is to take care of various events automtically as and when required and we need cloud service provider to manage compute resrources for us so that we are not worried when load of our application increases dynamically.
19.	Pay-as-you-go pricing	Cloud provider should offer a simple pay-as-you-go pricing where customers can pay for compute capacity with no long-term commitments.

2.7.3 Networking

	Requirement	Description
1.	Multiple network interface/instance	Cloud service should be able to support multiple (primary and additional) network interfaces.
2.	Multiple IP addresses/instance	Cloud service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network interface.
3.	Ability to move network interfaces and IPs between instances	Cloud service should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.
4.	Enhanced networking support	Cloud service should support capabilities such as single root I/O virtualization for higher performance (packets per second), lower latency, and lower jitter.
5.	Network traffic logging - Log traffic flows at network interfaces	Cloud service should support capturing information about the IP traffic going to and from network interfaces.
6.	Auto-assigned public IP addresses	Cloud service should be able to automatically assign a public IP to the instances.
7.	IP Protocol support	Cloud service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols.
8.	Use any network CIDR, including RFC 1918	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.
9.	Static public IP addresses	Cloud provider must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.
10.	Subnets within private network	Customer should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block.
11.	Subnet level filtering (Network ACLs)	Cloud service should support subnet level filtering – Network ACLs that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
12.	Ingress filtering	Cloud service should support adding or removing rules applicable to inbound traffic (ingress) to instances.

13.	Egress filtering	Cloud service should support adding or removing rules applicable to outbound traffic (egress) originating from instances.
14.	Disable source/destination checks on interfaces	Cloud service should support the ability to disable source/destination check on network interfaces. By default, compute instances perform source/destination checks.
15	Configure proxy server (NAT instance) at network level	Cloud service should support NAT instances that can route traffic from internal-only instances to the Internet.
16.	Site-to-site managed VPN service	Cloud service should support a hardware based & Software VPN connection between the cloud provider and customer data center.
17.	Virtual Network Peering	Cloud service should support connecting two virtual networks to route traffic between them using private IP addresses.
18.	Multiple VPN Connections per Virtual Network	Cloud service should support creating multiple VPN connections per virtual network
19.	BGP for high availability and reliable failover	Cloud provider should support Border Gateway Protocol. BGP performs a robust liveness check on the IPSec tunnel and simplifies the failover procedure that is invoked when one VPN tunnel goes down.
20.	Private connection to customer data centers	Cloud provider should support direct leased-line connections between cloud provider and a customer datacentre, office, or co-location environment, which in many cases can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
21.	DNS based global load balancing	Cloud service should support Load balancing of instances across multiple host servers.
22.	Load balancing supports multiple routing methods	Cloud service should support multiple routing mechanism including round-robin, failover, sticky session etc.
23.	Front-end Load Balancer	Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.
24.	Back-end Load Balancer	Cloud service should support an internal load balancer that routes traffic to instances within private subnets.

25.	Health checks - monitor the health and performance of application	Cloud service should support health checks to monitor the health and performance of resources.
26.	Integration with Load Balancer	Cloud service should support integration with load balancer.
27.	Low Latency	The CSP should be able to provide a upto 10GB network connectivity between the servers (if required).

2.7.4 Storage – Block Storage

	Requirement	Description
1.	Support for storage allocated as local disk to a single VM	Cloud provider should offer persistent block level storage volumes for use with compute instances.
2.	Storage volumes > 1 TB	Cloud provider should offer block storage volumes greater than 1 TB in size.
3.	SSD backed storage media	Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies.
4.	Expandable I/O support	Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
5.	Encryption using provider managed keys	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
6.	Encryption using customer managed keys	Cloud service should support encryption using customer managed keys.
7.	Durable snapshots	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.
8.	Ability to easily share snapshots globally	Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data centre migration, and disaster recovery.
9.	Attach more than one compute instance to a single volume	Cloud service should support adding more than one compute instance to a single storage volume in R/W mode so that many users can access and share a common data source.

10.	Consistent Input Output per second (IOPS)	Cloud service should support a baseline IOPS/GB and maintain it consistently at scale
11.	Annual Failure Rates <1%	Cloud service should be durable and support annual failure rates of less than 1%

2.7.5 Storage – Object Storage

	Requirement	Description
1.	Scalable object storage service	Cloud provider should offer secure, durable, highly-scalable object storage for storing and retrieving any amount of data from the web.
2.	Low cost archival storage with policy support	Cloud provider should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.
3.	Support for Server-side Encryption	Cloud service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data.
4.	Support for Server Side Encryption with a Key Management Service	We need encryption to secure our application . Cloud Provider should have service which can help us with overall encryption and key management process and at the same time we should be able to use our own keys based on application requirements.
5.	Object lifecycle management	Cloud Service should support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation/initial storage to deletion.
6.	Data Locality	Cloud provider should provide a strong regional isolation, so that objects stored in a region never leave the region unless customer explicitly transfers them to another region.
7.	Object change notification	Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).
8.	High-scale static web site hosting	Cloud service should be able to host a website that uses clientside technologies (such as HTML, CSS, and JavaScript) and does not require server-side technologies (such as PHP and ASP.NET).
9.	Object Versioning	Cloud Service should support versioning, where multiple versions of an object can be kept in one object storage account. Versioning protects against unintended overwrites and deletions.

10.	Flexible access-control mechanisms	Cloud service should support flexible access-control policies to manage permissions for objects.
11.	Audit logs	Cloud service should be able to provide audit logs on storage account including details about a single access request, such as the requester, storage account name, request time, request action, response status, and error code.
12.	Lower Durability offering	Cloud service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy.
13.	Parallel, multipart upload	Cloud service should allow uploading a single object as a set of
		parts where each part is a contiguous portion of the object's data and these object parts can be uploaded independently and in any order.
14.	CDN option for users	Cloud provider should offer a service to speed up distribution of static and dynamic web content.
15.	Strong Consistency	Cloud service should support read-after-write consistency for PUT operations for new objects.
16.	Storage gateway appliance for automated enterprise backups	Cloud provider should offer a storage gateway appliance for seamlessly storing on-premises data to the cloud.
17.	Accept large data loads through shipped physical media	Cloud provider should support moving large amounts of data into the cloud by bypassing the internet.
18.	Deliver large data exports through shipped physical media	Cloud provider should support moving large amounts of data out of the cloud by bypassing the internet.

2.7.6 Storage – File Storage

	Requirement	Description
1.	Simple, scalable file storage service	Cloud provider should offer a simple scalable file storage service to use with compute instances in the cloud.
2.	SSD backed storage media	Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads.
3.	Grow file systems to petabyte scale	Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections.

4.	Scalable IOPS and throughput performance (/TB)	Cloud service should support scalable IOPS and throughput performance at any scale.
5.	Sharable across thousands of instances	Cloud service should support thousands of instances so that many users can access and share a common data source.
6.	Fully elastic capacity (no need to provision)	Cloud service should automatically scale up or down as files are added or removed without disrupting applications.
7.	Highly durable	Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple data centres.
8.	Read-after-write consistency	Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).

2.7.7 Relational Database

	Requirement	Description
1.	Managed relational database service	Cloud provider should offer a service that makes it easy to set up, operate, and scale a relational database in the cloud.
2.	Support for MySQL	Cloud service should support the last two major releases of MySQL (versions 5.6, 5.5) as a database engine.
3.	Support for Oracle	Cloud service should support the last two major releases of Oracle (11g and 12c) as a database engine.
4.	Support for Microsoft SQL Server	Cloud service should support all the editions (Express, Web, Standard, Enterprise) of SQL Server 2012 as a database engine.
5.	Support for PostgreSQL	Cloud service should support the last two major releases of PostgreSQL (9.4.x, 9.3.x)

6.	Synchronous replication across data centres	Solution should be architected to run on cloud services offered from multiple data centre facilities to provide high availability with no interruptions in case of any disruptions to one of the data center facility. In case of failure, automated processes should move customer data traffic away from the affected area. The Cloud Service Provider should provide adequate bandwidth between the Data Centre Facilities to provide high availability.
7.	Read Replica support	Cloud service provider should support creating replicas of the database so that read queries can be offloaded to these replicas. This can be achieved using native DB capabilities.
8.	Manual Failover	Cloud service should support a manual failover of the DB instance from primary to a standby replica.
9.	Provisioned IO support	Cloud service should support the needs of database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
10.	Cross region Snapshots	Cloud service should support copying snapshots of any size between different cloud provider regions for disaster recovery purposes.
11.	Cross region Read Replica	Cloud service provider should support multiple replicas of DB instance offered from multiple data centre facilities to provide high availability and scalability with no interruptions in case of any disruptions to one of the data center facility. In case of DB master failure the failover to the secondary DB running in different data center should happen automatically without any manual intervention. The Cloud Service Provider should provide adequate bandwidth between the Data Centre Facilities to provide high availability.
12.	High Availability	Cloud Service should support enhanced availability and durability for database instances for production workloads.
13.	Point in time restore	Cloud service should support restoring a DB instance to a specific date and time.
14.	User snapshots and restore	Cloud service should support creating a DB snapshot and restoring a DB instance from a snapshot.
15.	Modifiable DB parameters	Cloud service should allow the DB parameter to be modified.
16.	Monitoring	Cloud service should allow monitoring of performance and health of a database or a DB instance.

17.	Encryption at rest	Cloud service should support encryption using the industry standard AES-256 encryption algorithm to encrypt data.

2.7.8 Non-Relational Database

	Requirement	Description
1.	Scalable, fast and flexible NoSQL database service	Cloud provider should offer a fast and flexible NoSQL database service for applications that need consistent, single-digit millisecond latency at any scale.
2.	Replication	Cloud service should support automatic replication of data across multiple physical data centres in a region to provide high availability and data durability.
3.	Performance/ Latency	Non-relational databases are required for use case where high concurrency and low latency is required
4.	Key-value Data Model support	Cloud service should support key value data structure where the primary key is the only required attribute for items in a table and uniquely identifies each item.
5.	Document Data Model with JSON support	Cloud service should support storing, querying, and updating JSON documents.
6.	Tenable scaling	Cloud service should support seamless throughput and storage scaling.
7.	Secondary Indexes	Cloud service should support secondary indexes. Secondary indexes are indexes that contain hash or hash-and-range keys that can be different from the keys in the table on which the index is based.
8.	Streams	Cloud service should support streams. Stream is an ordered flow of information about changes to items.
9.	Cross region replication	Cloud Service should support cross-region replication to automatically replication data across multiple regions.
10.	Database triggers	Cloud Service should support database triggers - pieces of code that quickly and automatically respond to data modification in the tables.
11.	Strong consistency, Atomic counters	Cloud service should support strong consistency for read operations to make sure users are always reading the latest values.
12.	Integrated Monitoring	Cloud service should support monitoring of request throughput and latency for database tables, among other metrics.

13.	Integration with data warehouse	Cloud service should support integration with a data warehouse for advanced business intelligence capabilities.
14.	Hadoop Integration	Cloud service should support integration with a Hadoop framework to perform complex analytics on large datasets.

2.7.9 Security and administration

	Requirement	Description
1.	Control access to your cloud resources at a granular level	Cloud provider should offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device.
2.	Utilize multi-factor authentication when accessing cloud resources	Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.
3.	Identify last access user log and remove inactive user	Cloud service should support reporting a user's last access details.
4.	Policy validation to ensure policies match intentions	Sol need strong access control and audit ability of objects
5.	Directory as a service	Cloud provider should support setting up a stand-alone directory in the cloud or connecting cloud resources with existing on-premises Microsoft Active Directory.
6.	User and Group management	Cloud service should support features such as user and group management.
7.	Integration with your existing on-premises Active Directory	Cloud service should integrate with existing on-premise Active Directory.
8.	Self-service password reset for cloud users	Cloud service should allow users to reset their password in a self-service manner.
9.	Managed service to create and control the encryption keys used to encrypt your data	Cloud provider should offer a service to create and control the encryption keys used to encrypt user data.
10.	Audit of all action on keys	Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.

11.	Key Durability	Cloud service should support durability of keys, including storing multiple copies to ensure keys are available when needed.
12.	Web service to record API calls and deliver log files	Cloud provider should offer a service to record history of API calls and related events for a user account.
13.	Receive notification of API activity	Cloud service should support notifications when new log files are available.
14.	Durable and inexpensive log file storage	Cloud service should support storing log files in a durable and inexpensive storage solution.
15.	Choice of partner solution	Cloud service should support a variety of 3rd party solutions.
16.	Aggregation across multiple accounts and multiple Regions for ease of use	Cloud provider should have service to capture log for each API call that is made to SOL cloud account. This is required for audit purpose.
17.	Managed service for resource inventory, configuration history & change notifications	Cloud provider should offer a service that provides resource inventory, configuration history, and configuration change notifications to enable security and governance.
18.	Automatically records a resource's configuration when it changes	Cloud service should automatically record a resource configuration when it changes and make this information available.
19.	Examine the configuration of your resources at any single point in the past	Customer should be able to obtain details of what a resource's configuration looked like at any point in the past using this cloud service.
20.	Receive notification of a configuration change	Cloud service should notify every configuration change so customers can process these notifications programmatically.
21.	Create and manage catalogue of pre-approved services for use	Cloud provider should offer the ability to create and manage catalogues of IT services that are approved for use.

2.7.10 Security and administration

	Requirement	Description
1.	• 3rd party Assurance Programs • SOC1 / ISAE 3402 • SOC2 / SOC3 • ISO 27001 • ISO 9001 • PCI DSS Level 1 • FISMA • FIPS 140-2 CSA	Cloud provider should meet a broad set of international and industry-specific compliance standards: ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, and SOC 3.

2.7.11 Deployment and Management

	Requirement	Description
1.	Service to quickly deploy and manage applications in the cloud	Cloud provider should offer a service to quickly deploy and manage applications in the cloud by automatically handling the deployment, from capacity provisioning, load balancing, autoscaling to application health monitoring.
2.	Supported Platforms • Java • Ruby • PHP • Node.js • Google Go • NET • Python	Cloud service should support a wide variety of platforms from Java and .NET to Google Go.
3.	Supported OS • Windows • Linux • any OS in Docker	Cloud Service should support Windows, Linux, and Docker containers.
4.	Deployment Mechanism • Git • Zip • Eclipse • Visual Studio	Cloud service should support various deployment mechanisms, including a Git repository, or an integrated development environment (IDE) such as Eclipse or Visual Studio.
5.	Support for SSL connections	Cloud service should support SSL connections.

6.	Application source versioning	Cloud service should support application source versioning. This would be useful for applications that have been updated and need to be redeployed.
7.	Auto scaling	Cloud service should support automatically launching or terminating instances based on the parameters such as CPU utilization defined by users.
8.	Swap virtual IP between staging and production environments	Cloud service should support swapping IP addresses between staging and production environments so that a new application version can be deployed with zero downtime.
9.	Integration with caching solution	Cloud service should be integrated with a caching solution such as Redis cache.
10.	Service to create a collection of related resources and provision them using a template	Cloud provider should offer a service to create a collection of related resources and provision them in an orderly and predictable fashion using a template.
11.	Single JSON based template to declare your stack	Cloud service should use a template, a JSON-format, text-based file that describes all the resources required for an application. The resources in the template should be managed as a single unit.
12.	Allow parameterization and specific configurations	Cloud service should support parameterization for specific configuration.
13.	Integration with the portal	Cloud service should be integrated with the portal.

2.7.12 Application Services

	Requirement	Description
1.	Search service	Cloud provider should offer a search service in the Cloud that makes it simple and cost-effective to set up, manage, and scale a search solution for websites or applications.
2.	Queuing service	Cloud provider should offer a fast, reliable, scalable, fully managed message queuing service.
3.	Notification service	Cloud provider should offer a fast, flexible, fully managed push notification service that lets users send individual messages or to fan-out messages to large numbers of recipients.
4.	Bulk email delivery service	Cloud provider should offer a cost-effective outbound-only email-sending service.

5.	Media transcoding service	Requirement is to have a managed service from cloud provider that enables media transcoding for media.

2.7.13 Hybrid Integration

2.7.14

	Requirement	Description
1.	Hardware-based virtual private networking connection to cloud resources	Cloud provider should be able to extend customer's data center to the cloud and enable communication with their own network over an IPsec VPN tunnel.
2.	High speed, low latency, dedicated connectivity between on-premises & cloud	Cloud provider should provide mechanisms to establish private connectivity between the cloud environment and a customer data centre, office, or colocation environment.
3.	Automated VM import functionality	Cloud provider should allow customers to import VMs from a virtualization environment such as Citrix Xen, Microsoft Hyper-V, or VMware vSphere.
4.	Automated VM export functionality	Cloud provider should allow customers to export instances to their on-premises virtualization environments.
5.	Integrate with on-premises Active Directory	Cloud service should integrate with existing on-premise Active Directory.
6.	Use any IP address range, including RFC 1918	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.
7.	Highly durable, automatic data replication, and recovery service from on-premises	Cloud provider should offer a service to automatically replicate data from on-premises to cloud for disaster recovery purposes.
8.	Backup service to back up on-premises servers	Cloud provider should offer a service with ability to take regular and scheduled back of on-premises servers.
9.	Utilize multi-factor authentication when accessing cloud resources	Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.
10.	Support from 3rd party management and monitoring tools	Cloud provider should offer management and monitoring plugins for management solutions from multiple vendors.

11.	App management service to deploy and operate apps in the Cloud or own data centre	Cloud provider should offer a service to automate operational tasks like software configurations, package installations, and database setups for servers running on-premises or in the cloud.
12.	Service to automate code deployments to cloud and on-premises	Cloud provider should offer a service that automates code deployments to servers running on-premises or in the cloud.

2.7.15 Other Technical Requirements

	Requirement	Description
1.	Financial analysis recommendation engine	SOL needs clear view of their provisioned and consumed cloud services though an automated way so that there is full transparency of utilization . Based on usage and recommendation Sol would be able to optimize resource utilization and save cost by right sizing and architecture.
2.	Content delivery network	Cloud Service Provider must offer a service for global content delivery networking. The CDN service must be offered in self-service fashion with all maintenance offered by the provider.
3.	Relational DBaaS	Cloud Service provider must offer a relational database as a service (DBaaS), provided as a fully automated, self-service turnkey offering. In this service, the customer should not have access to the underlying instance, and the database maintenance must be done entirely by the provider. At a minimum, the service must support two open-source database (either MySQL and PostgreSQL) and two enterprise database (either Microsoft SQL Server or Oracle). CSP must offer relational DBaaS in a locally redundant fashion, meaning that the customer database is automatically replicated across multiple data centers within a single geography.
4.	Customer VPN connectivity	Cloud Service Providers must allow customers to access the cloud service via an IPsec VPN tunnel or Secure Sockets Layer (SSL) VPN tunnel over the public Internet. This must be a self-service capability from the provider side, although customers will have to make configurations on their end.

5.	Instance-encrypted volumes Provider-enabled encryption services	High level security and encryption is expected to secure data. Sol should be able to secure data at rest using encryption. Cloud provider needs to have a service for it. We are looking for self service capabilities through a console or dashboard as well as command line interface so that we can use it without any cloud providers intervention.
6.	Large instance support	Large instance support: Providers must offer customers instances with a large number of processor cores and memory for processor- or memory-intensive use cases. The provider must be able to provide instances that support at 128 vCPUs and 1952 GB of RAM.

2.8 Support

	Requirement	Description
1.	Service Health Dashboard	Cloud provider should offer a dashboard that displays up-to-the minute information on service availability of various cloud service provided by the cloud provider "Its required so that Sol can themselves check service availability at any time with no intervention of cloud provider.
2.	365-day service health dashboard and SLA history	Cloud provider should offer 365 days' worth of Service Health Dashboard (SHD) history.
3.	Service to compare resource usage to best practices	Cloud provider should offer a service acts like a customized cloud expert and helps provision resources by following best practices.
4.	Monitoring Tools	Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health.
5.	Governance and Compliance	Sol needs capability to standardize their cloud deployments and maintain a compliance across deployment to secure and have better control over our cloud environment.
6.	Audit Trail	Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing

2.9 Backup & Restore

In order to safeguard the data hosted on cloud, Bidder should ensure regular onsite backups of the cloud data at client DR site. There may be cost implications for the same.

1. The backup should be incremental & differential.
2. RPO (Recovery Point Objective) for onsite backup must be less than 30 mins and for On Cloud backup must be 15 mins.
3. RTO (Recovery Time Objective) for onsite backup and for On-Cloud backup must be 30 mins.

NOTE: Above specifications are desirable. The Bidders can add their proposed specifications in case of any additional requirement

SECTION III

INSTRUCTION TO BIDDERS

A. GENERAL

2.1 GENERAL TERMS OF BIDDING

a) The bid should be submitted in the format exactly as per Appendix A-1 and Appendix A-2. The amount should be indicated in words and figures clearly in Appendix A-2.

b) Bidders shall bear all costs associated with the preparation and submission of bid. SOL shall not in any case be responsible or liable for these costs.

2.2 ELIGIBILITY CRITERIA

a) The bidder should be a legally valid legal entity either in the form of a Limited Company or Private Limited Company registered under the Companies Act, 1956 and in operation in India for minimum of three (3) years as on 31 March 2019.

b) The bidders should have authorization from Cloud Service Provider (CSP) that they have affiliation with the CSP for the service as on Bid submission date and can participate in the bid and shall provide service only from that CSP under this bid.

c) The bidder should have provided Service of Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) to at least 03 different clients of a minimum value of Rs 10 lakh per year to each client during last 02(Two) years ending 31st March 2019 in India as on bid submission date with Governments Departments/PSUs/Autonomous Bodies or any reputed organizations.

d) The annual turnover of the bidders should not be less than Rs.1 (One) crore for the years ended March 2017, March 2018 and March 2019.

e) The Bidder should have minimum of Five (05) on roll resources that have cloud certification from any CSP as on Bid submission date.

f) The Bidder must have on its roll at least 10 Technically qualified professionals with combinations in the following fields
Technically qualified professionals with combination in the
Following fields:
a) System integrations
b) Virtualization
c) Security
d) Experience in implementing the cloud solutions as on 31 march, 2019.

g) The bidders should be registered with Income Tax departments/Goods and
Service Tax department.

h) The bidder should have not been black listed by Government Department/ PSUs /Autonomous Bodies.

2.3 EARNEST MONEY DEPOSIT (EMD)

The bidders shall submit an EMD of Rs.60,000/- (Sixty Thousand) only in demand draft, from any nationalized bank or scheduled commercial bank in favour of Officer on Special Duty, School of Open Learning, University of Delhi to Section Officer (General) in Room No. 206 on or before the date of submission of bid in a sealed cover. The validity period of the Bank Guarantee shall be three months. However, the bidder will have to upload scanned copy of EMD with technical bid.

The EMD shall be forfeited, if;

i) The bidder withdraws the bid before expiry of its validity.

ii) Successful bidder does not accept the order or fails to enter into a contract within validity of offer.

iii) The tender with no EMD shall be summarily rejected.

iv) EMD of successful bidder will be returned on receipt of performance security.

v) In case of unsuccessful bidder, the EMD will be refunded without interest.

2.4 VALIDITY OF BIDS

The BIDs shall be valid for a period of not less than120 (one hundred and twenty) days from the Bid Due Date. The validity of Bids may be extended by mutual consent of the respective bidders and the SOL.

2.5 VERIFICATION AND DISQUALIFICATION

a) SOL reserves the right to verify all statements, information and documents submitted by the bidder.

b) SOL reserves the right to reject any bid and appropriate EMD if, at any time, a material misrepresentation is made or uncovered**.**

B. DOCUMENTS

(a) CONTENTS OF DOCUMENTS	
The Tender Document consists of the following	
(i)	**E-Tender Notice**
(ii)	**Introduction – Section I**
(iii)	**Scope of work – Section II**
(iv)	**Instruction to bidders – Section III**
(v)	**Commercial conditions – Section IV**
(vi)	**Service Level Targets – Section V**
(vii)	**Check List – Section VI**
(viii)	**Technical Bid – Appendix : A-1**
(ix)	**Financial Bid – Appendix : A-2**

(x)	**Undertaking regarding Blacklisting – Appendix: B**
(xi)	**Performa for Annual Turnover – Appendix C**
(xii)	**Tender Acceptance Letter – Appendix D**
(xiii)	**Form of Performance Bank Guarantee : Appendix – E**
(xiv)	**Form of Agreement – Appendix - F**

c)AMENDMENT OF TENDER DOCUMENT

At any time prior to the deadline for submission of bids, the SOL may for any reason, whether at its own initiative or in response to a clarification requested by the prospective bidders, modify the bidding documents by amendment. The amendment will be uploaded on CPP Portal http://eprocure.gov.in/eprocure/app for the benefit of all the prospective bidders.

d) PREPARATION AND SUBMISSION OF BIDS

FORMAT AND SIGNING OF BIDS

i) The bidders shall provide all the information sought under this Tender Document. SOL will evaluate only those bids that are received on-line in the required formats and complete in all respects; and EMD and other documents are received in hard copy.

ii) The tender should be digitally signed on each page by the authorized signatory of the bidder.

2.6 DOCUMENTS COMPRISING TECHNICAL AND FINANCIAL BID

The bidder shall submit the Technical and Financial Bid online through CPP Portal http://eprocure.gov.in/eprocure/app comprising of the following documents as appropriate

A	**TECHNICAL BID-Appendix A-1 digitally signed**
(a)	Appendix: A-1
(b)	Scanned copy of Certificate of a legally valid entity either in the form of a Limited Company or a Private Limited Company registered under the Companies Act, 1956
(c)	Scanned copy of document showing authorization letter issued by the CSP that the MSP is able to sell
(d)	Scanned copies of Experience certificate from Government departments/ PSUs/ Autonomous Bodies or any reputed organizations. in last three financial years ending 31 March 2019 for providing service of platform as a service (PaaS) or infrastructure as a service (IaaS) to atleast 3 (Three) different clients of a minimum value of Rs. 10 lakh per year to each client in India.

(e)	Scanned copy of the annual turnover of the bidders should not be less than Rs 1 (One) crore for the years ended March 2017, March 2018 and March 2019 duly certified by Chartered Accountant.
(f)	Scanned copies of valid CSP Certification.
(g)	Self-Certification by the authorized signatory with clear declaration of the number of staff – year wise, level/designation wise.
(h)	Scanned copy of EMD.
(i)	Scanned copy of PAN CARD.
(j)	Scanned copies of declaration of non-blacklisting.
(k)	Scanned copy of GST Registration Certificate.
(l)	Copy of Board Resolution/power of Attorney/Authorization letter indicating that the person signing the Bid has the required authority to sign on behalf of the Bidder.
(m)	Tender Acceptance Letter

B FINANCIAL BID-

Financial bid format is provided with Appendix-A2 along with this tender document at https://eprocure.gov.in. Bidders are advised to write/quote their offered rates in the permitted column in the financial bid. **Bidder shall not tamper/modify price bid template in any manner**. In case if the same is found to be tempered/modified in any manner, tender will be completely rejected and EMD would be forfeited. The bidders have to quote the rate keeping in view the specifications and terms and conditions of tender.

1. The rates shall be quoted in Indian Rupee only.
2. The rates will be inclusive of GST.
3. In case of any discrepancy/difference in the amounts indicated in figures and words the amount in words will prevail and will be considered.

2.7 BID DUE DATE

The technical and financial bid shall be submitted on CPP Portal http://eprocure.gov.in/eprocure/app on 15/11/2019 at 5.30 P.M.. Similarly, physical submissions of documents will also be completed by the same date and time.

ONLINE OPENING OF BIDS

a) Opening of bids will be done through on-line process**.**

b) SOL shall on-line open Technical Bids on 18/11/2019 at 11:30 a.m. hrs. IST, in the presence of the authorized representatives of the bidders, who choose to attend.

c) Technical Bid of only those bidders shall be on-line opened whose digitally signed documents listed at **clause 2.6 (A)** have been received with Appendix A-1. The SOL will subsequently examine and evaluate the Bids in accordance with the provisions of this document.

2.8 REJECTION OF BIDS

a) Notwithstanding anything contained in this document, the Officer on Special Duty, SOL reserves the right to reject any bid and to annul the Bidding Process and reject all bids at any time without any liability or any obligation for such acceptance, rejection or annulment, and without assigning any reason, therefore. In the event that the SOL rejects or annuls all the bids, it may, in its discretion, invite all eligible bidders to submit fresh bids hereunder.

b) The SOL reserves the right not to proceed with the bidding process at any time, without notice or liability, and to reject any Bid without assigning any reasons.

2.9 CORRESPONDENCE WITH THE BIDDER

SOL shall not entertain any correspondence with any bidder in relation to acceptance or rejection of any bid.

C. EVALUATION OF BIDS

TESTS OF RESPONSIVENESS

Prior to evaluation of Technical Bids, SOL shall determine whether each Technical

Bid is responsive to the requirements of this document. A Technical Bid shall be considered responsive only if:

(a) Bid is received online as per the format at Appendix A-1 with digitally signed documents listed at clause 2.6 (A).

(b) It is accompanied by EMD.

(c) It is not non-responsive in terms of this document.

2.10 OPENING AND EVALUATION OF FINANCIAL BIDS

The SOL shall inform the venue and time of online opening of the Financial Bids to the technically responsive bidders (Technically Qualified Bidders) through their email id and state the date of opening on the e-procurement portal. SOL shall online open the Financial Bids only of Technically Qualified Bidders on the due date and time in the presence of the authorized representative of the Technically Qualified Bidders who may choose to attend. SOL reserves the right to reject any BID which is non-responsive and no request for alteration, modification, substitution or withdrawal shall be entertained by the SOL in respect of such BID.

2.11 DETERMINATION OF RATES

SOL shall determine the lowest rates based on the financial bids opened. SOL has the right to reject any rate it considers un-workable. The financially determined rates will become the approved rates ("Approved Rates").

2.12 OFFER OF APPROVED RATE TO FINANCIALLY QUALIFIED BIDDER

The SOL shall offer the approved rates to the Technically Qualified Bidder for acceptance of the rates and conditions of contracts.

2.13 PLACEMENT OF WORK ORDER

Upon receipt of acceptance of rates and performance security, SOL shall place order on successful bidder**.**

2.14 CONTRACT PERIOD

The contract shall be valid for one year from the date of award of work which can further be extended for one more year on the same rates, terms & conditions if the performance is found satisfactory in the discretion of OSD, SOL. The OSD, SOL reserves the right to curtail or extend the validity of contract.

2.15 SIGNING OF SERVICE LEVEL AGREEMENT

The successful bidder shall sign an Agreement before commencement of work in Appendix - F

SECTION –IV

COMMERCIAL CONDITIONS OF CONTRACT

1 APPLICATION

The general conditions shall apply in contracts made by the Client for the procurement of Goods / services.

2 STANDARDS

The services provided under this contract shall conform to the standards prescribed in the Scope of Work given in SECTION II.

3 PERFORMANCE BANK GUARANTEE (PBG)

a) The successful bidder shall at his own expense deposit with the Section Officer(General)), SOL within fourteen (14) working days of the date of notice of award of the contract or prior to signing of the contract whichever is earlier, an unconditional and irrevocable Performance Bank Guarantee (PBG) from a Nationalized Bank/ Scheduled Commercial Bank in the name of Officer on Special Duty, SOL payable at Delhi, for the due performance and fulfillment of the contract by the bidder. This PBG will be for an amount equivalent to 10 (ten) % of contract value in the prescribed format given in **Appendix-E.** All incidental charges whatsoever such as premium; commission etc. with respect to the PBG shall be borne by the bidder. The PBG shall be valid beyond 60 days of completion of work and extended period if any. The PBG may be discharged/ returned by SOL upon being satisfied that there has been due performance of the obligations of the bidder under the contract. However, no interest shall be payable by SOL on the PBG.

b) In the event of the bidder being unable to service the contract for reasons not found to be reasonable and satisfactory by the competent authority, the SOL would invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of the Authority under the contract in the matter, the proceeds of the PBG shall be payable to SOL as compensation for any loss resulting from failure of the bidder to perform/ comply its obligations under the contract. The Section Officer (General), SOL 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.

4 CONFIDENTIALITY

a) The Bidder shall further ensure that the information given by the SOL, University of Delhi is not disclosed to any person, firm body, corporate and/or authority and make every effort to keep the above information strictly confidential. All such information shall remain the absolute property of the School of Open Learning, University of Delhi.

b) Information relating to the examination, clarification, evaluation and recommendation for the bidders shall not be disclosed to any person who is not officially concerned with the process or is not a retained professional advisor advising the SOL in relation to, or matters arising out of, or concerning the bidding process.

5 SOL's RIGHT TO TERMINATE BID PROCESS

The Officer on Special Duty, SOL reserves the right to accept any bid, and to cancel/ abort the tender process and reject all bids at any time prior to award of Contract without thereby incurring any liability to the affected successful Bidder or any obligation to inform the affected successful Bidder of the grounds for SOL's action.

6. OBLIGATION OF THE SELECTED MSP

The Bidder selected for implementing clouding service shall perform the services and carry out its obligations under the Contract with due diligence and efficiency.

7. PAYMENT TERMS

- Payment shall be made in quarterly Basis.

h) Payment shall be made in INR (irrespective of the invoices raised by CSP in different currency) and the prices mentioned in the contract should only be valid for the entire contract period. Any increase in prices during the period of contract shall be to the Bidder's account. In case of reduction in the prices, SOL shall take the benefit of reduction in price from the date of reduction in prices. Any price increase at the end of year 1 will be notified separately to SOL.

- Adherence to timelines is critical for the success of the project.
- No advance payment shall be made for any activity.
- SOL will release the payment within 15 days of submission of 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 SLT Criteria. SOL shall be entitled to delay or withhold the payment of a disputed invoice or part of it delivered by Bidder, when SOL disputes such invoice or part of it, provided that such dispute is bonafide. No interest shall be paid by SOL in case of delay of Payments.
- No payment made by SOL herein shall be deemed to constitute acceptance by SOL of the system or any service
- 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.
- All payments shall be made for the corresponding to the goods or services actually delivered, installed, or operationally accepted, as per the Contract Implementation Schedule, at unit prices and in the currencies specified in the Commercial Bids.
- All Invoices should be supported with the full set of service level reports.
- For payment, the invoice with relevant documents such as Operational Acceptance Certificate should be submitted to the Officer-on-Special Duty, SOL.

- Payments shall be subject to deductions of any amount as per terms and conditions of this tender. Further, all payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the income - Tax Act, 1961 and any other taxes.
- All payment shall be made after adjusting the penalty deductible, if any.
- The SOL shall make above payment directly in the Account of successful bidder. To Make following information in respect of their Bank Account :

  Name of Bank and address of Branch
  Their Bank Account Number
  IFS Code of the Branch for RTGS Transfer
  - The SOL shall not be liable for payment of any interest on delayed payment.

(d) PENALTIES

Time is the essence of Agreement and the delivery dates are binding on the Implementation Agency. In the event of delay or any gross negligence in implementation of Project before Go-live, for causes solely attributable to the implementation Agency, in meeting the deliverables, SOL shall be entitled to recover from the Implementation Agency as agreed, liquidated damages, a sum of 0.5% of the value of the deliverables which suffered delay or gross negligence foe each completed month or part thereof subject to a limit of 5% of the Invoice value. The right to claim any liquidated damages shall be without prejudice to other rights and remedies available to SOL under the contract or law.

(e) OUTSOURCING OF WORK

The successful Bidder shall not outsource the work of cloud service to any other agency.

(f) TERMINATION FOR INSOLVENCY

The SOL may at any time terminate the contract by giving written notice of 30 days to the successful Bidder, without any compensation to the Bidder, if the it becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the SOL.

(g) TERMINATION FOR DEFAULT

Default is said to have occurred

If the successful bidder fails to deliver any or all of the systems within the period (s) specified in the contract, or within any extension granted by SOL pursuant to conditions of contract clause or if the complete the work of cloud Service in accordance with the plan within the time period(s) specified in the contract or any extension thereof granted by the SOL.

If the successful bidder fails to perform any other obligation(s) under the contract /work order. If the successful bidder fails to comply with instructions of the SOL with respect to improving the quality of cloud services

(h) REMEDIAL MEASURES

If the Successful bidder, in either of the above circumstances, does not take remedial steps within a period of 15 days after receipt of the default notice from the authority, (or takes longer period in spite of what the Officer on Special Duty, SOL may authorize in writing), the SOL may terminate the contract / work order in whole or in part. In addition to above, the SOL may at its discretion may transfer upon such terms and in such manner, as it deems appropriate, work order for similar service to other agency and the defaulting agency shall be liable to compensate the SOL totally for any extra expenditure involved to complete the scope of work.

(i) FORCE MAJEURE

If, at any time, during the continuance of this contract, the performance in whole or in part by either party of any obligation under this contract in prevented or delayed by reasons of any war of hostility, acts of the public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics, quarantine restrictions, strikes, lockouts or act of God (hereinafter referred to as events) provided notice of happenings of any such eventuality is given by either party to the other within 21 days from the date of occurrence thereof, neither party shall be reason of such event be entitled to terminate this contract nor shall either party have any claim for damages against other in respect of such non-performance or delay in performance, and deliveries under the contract shall be resumed as soon as practicable after such an event come to an end or cease to exist, and the decision of the Officer on Special Duty ,SOL as to whether the deliveries have been so resumed or not shall be final and conclusive. Further that if the performance in whole or part any obligation under this contract is prevented or delayed by reasons of any such event for a period exceeding 60 days, either party may, at its option, terminate the contract.

(j) SET OFF

Any sum of money due and payable to Successful Bidder (including Performance Security Deposit refundable to the firm) under this contract may be appropriated by Officer on Special Duty, SOL or any other person(s) contracting through SOL and set off the same against any claim of the SOL or such other person or person(s) for payment of sum of money arising out to this contract or under any other contract made by Successful Bidder SOL or such other person(s) contracting through the SOL

(k) CONFLICT OF INTEREST

Bidder shall furnish an affirmative statement as to the existence of, absence of, or potential for conflict of interest on the part of the bidder or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with the SOL. Additionally, such disclosure shall address any and all potential element (time frame for service delivery, resource, financial or other) that would adversely impact the ability of the bidder to complete the requirements as given in the Tender Notice.

(l) ARBITRATION

All disputes, differences and questions arising out of or in any way touching or concerning this agreement or subject matter thereof or the representative rights, duties or liability of the parties shall be referred to the sole arbitration of the Officer on Special Duty ,SOL or any person nominated by him. The arbitration shall be in accordance with the Arbitration and Conciliation Act, 1996. The arbitrator shall be entitled to extend

the time of arbitration proceedings with consent of the parties. No part of the agreement shall be suspended on the ground of pending arbitration proceedings.

(m) COURT JURISDICTION

It is also condition of this contract that the court which has territorial jurisdiction over Delhi shall have the absolute jurisdiction for adjudicating any difference or disputes arising out of this contract to the exclusion of all other court

SECTION V

SERVICE LEVEL TARGETS (SLT)

Bidder shall provide an uptime of 99.95% for the provisioned cloud services, which shall be calculated on monthly basis. The Uptime is equal to total contracted hours in a month less downtime. The Downtime is the time between the non-availability of services and time of restoration of services within the contracted hours. For Service Levels purpose a month will be treated as 30 days. If the bidder fails to maintain guaranteed uptime of 99.95% on monthly basis, SOL shall impose penalty. If the uptime is below 95%, the SOL shall have full right to terminate the contract.

Service Levels

S.N	Service Level Objective	Measurement / Methodology	Target/Service Level	Penalty
1.1.1 Availability/Uptime				
1.	Cloud Service Resources	Availability will be measured for each of the underlying component (eg. VM, Storage, OS, VLB, Security components) provisioned in the cloud. Measurement with the help of SLA reports provided by MSP	CSP should provide minimum of 99.9% read / write access to data stored on the cloud storage.	<100% – >=99.95% (None) <99.95% – >=99% (5% of periodic payment) <99% (10% of periodic payment)
2.	Network Connectivity	Availability will be measured for each of the network links provisioned in the cloud.	CSP should provide minimum 99.95% uptime for dedicated network connection as well S2S type connectivity from Cloud data center	<100% – >=99.95% (None) <99.95% – >=99% (5% of periodic payment) <99% (10% of periodic payment)
3.	Notifications	Availability will be measured for each of the service via Infra Management Tool provided by the MSP	CSP should provide minimum 99.9% uptime SLA for execution of alert rules, trigger and deliver notifications	<100% – >=99.95% (None) <99.95% – >=99% (5% of periodic payment) <99% (10% of periodic payment)

4.	Security	Availability will be measured for each of the service via Infra Management Tool provided by the MSP	CSP should provide minimum 99.9% availability of security and monitoring services deployed on the cloud resources	<100% – >=99.95% (None) <99.95% – >=99% (5% of periodic payment) <99% (10% of periodic payment)
5.	DDoS	Availability will be measured for each of the service via Infra Management Tool provided by the MSP	CSP should ensure minimum 99.99% uptime SLA for DDoS enabled for cloud resources	<100% – >=99.95% (None) <99.95% – >=99% (5% of periodic payment) <99% (10% of periodic payment)
6.	Firewall	Availability will be measured for each of the service via Infra Management Tool provided by the MSP	CSP should ensure minimum 99.95% uptime SLA for firewall services provided on cloud	<100% – >=99.95% (None) <99.95% – >=99% (5% of periodic payment) <99% (10% of periodic payment)
7.	Multi Factor Authentication	Availability will be measured for each of the service via Infra Management Tool provided by the MSP	CSP should ensure minimum 99.9% uptime SLA for MFA services enabled on cloud	<100% – >=99.95% (None) <99.95% – >=99% (5% of periodic payment) <99% (10% of periodic payment)

1.1.2 Service Levels for Disaster Recovery				
10.	Recovery Time Object (RTO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RTO <=2 hours	5% of Periodic Payment per every additional 2 hours of downtime
11.	Recovery Point Object (RPO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RPO <= 30 mins	5% of Periodic Payment per every additional 1 (one) hours of downtime

1.1.3 Security Incident and Management Reporting				
12.	Percentage of timely incident report	Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e. month). Incident Response - CSP shall assess and acknowledge the defined incidents within 1 hour after discovery.	95% within 1 hour	<100% – >=95 % (None) <95% – >=90% (1% of periodic payment) <90% – >=85% (2% of periodic payment) <85% (5% of periodic payment)
13.	Percentage of timely incident resolution	Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (month) over the total number of defined incidents to the cloud Service within a predefined period (Month). Measured from Incident Reports	95% to be resolved within 1 hour	<100% – >=95 % (None) <95% – >=90% (1% of periodic payment) <90% – >=85% (3% of periodic payment) <85% (5% of periodic payment)
1.1.4 Support Channels – Incident and Helpdesk				

14.	Response Time	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 15minutes	<100% – >=95 % (None) <95% – >=90% (1% of periodic payment) <90% – >=85% (3% of periodic payment) <85% (5% of periodic payment)
15.	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 98% of the incidents should be resolved within 30 minutes of problem reporting	<100% – >=98 % (None) <98% – >=90% (1% of periodic payment) <90% – >=85% (3% of periodic payment) <85% (5% of periodic payment)
16.	Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting AND 95% of Severity 3 within 16 hours of problem reporting	<100% – >=95 % (None) <95% – >=90% (1% of periodic payment) <90% – >=85% (2% of periodic payment) <85% (3% of periodic payment)

Note:

1. Periodic Payments means MONTHLY payments.
2. Severity Levels: Below severity definition provide indicative scenarios for defining incidents severity. However, ZNet will define / change severity at the time of the incident or any time before the closure of the ticket based on the business and compliance impacts.

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

SECTION VI

CHECK LIST

This check list is to help the bidders ensure that bids are complete.

Mention Page Numbers

S. No.	Details	Documents to be uploaded (Scanned Copy)	Attached (Y/N)	Page No.
1	Certificate of a legally valid entity either in the form of a Limited Company or a Private Limited Company registered under the Companies Act, 1956	Certificate of incorporation/ registration		
2	The bidders should have authorization from Cloud Service Provider (CSP) that they have affiliation with the CSP for the service as on Bid submission date and can participate in the bid and shall provide service only from that CSP under this bid.	Certificate/authorization letter issued by CSP that the MSP is able to resell		
3	The annual turnover of the bidders should not be less than Rs.1 crore for the years ended March 2017, March 2018 and March 2019.	In Appendix- D		
4	The bidder should have provided Service of Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) to at least 03 different clients of a minimum value of Rs 10 lakh per year to each client during last 02(Two) year in India as on bid submission date with Governments departments/PSUs/Autonomous Bodies or any reputed organizations.	Copies of the Purchase orders with performance certificates from clients.		
5	The Bidder should have minimum of Five (05) on roll resources that have cloud certification from any CSP as on Bid submission date	Copies of valid CSP Certification		
6	The Bidder must have on its roll at least 10 Technically qualified professionals with combinations in the following fields Technically qualified professionals with combination in the following fields a) System integrations b) Virtualization c) Security d) Experience in implementing the cloud solutions as on 31 march, 2019.	Self-Certification with clear declaration of the number of staff – year wise, level/designation wise.		

7	GST Registration Certificate	Self Certified		
8	PAN Card	Self Certified		
9	Declaration regarding non- blacklisting of the firm	Appendix - C		
10	EMD (Demand draft only)	Copy		
11	The bid must be signed by a person duly authorized to bind the tenderer of the contract	Copy of Authorization letter		
12	Tender Acceptance letter	Appendix-D		

APPENDIX-A-1

Letter for Technical Bid

(On letter head of the bidder)

Dated:

To

Officer on Special Duty,
School of Open Learning
5, Cavalry Lane,
University of Delhi,
Delhi-110007

Sub: Technical Bid for selection of Managed Service Provider (MSP) for implementation of cloud services School of Open Learning

Dear Sir,

With reference to your Tender Document dated ……., we, having examined the document and understood its contents, hereby submit our Technical Bid for qualification for the aforesaid work. The bid is unconditional and unqualified.

2. We acknowledge that the SCHOOL OF OPEN LEARNING (SOL) will be relying on the information provided in this letter and the documents accompanying it. We certify that all information provided in the letter and in Annex I is true and correct; nothing has been omitted which renders such information misleading; and all documents accompanying the letter are true copies of their respective originals.

3. This statement is made for the express purpose of qualifying as a bidder selection of Managed Service Provider (MSP) for implementation of cloud services in SOL.
4. We shall make available to the SOL any additional information it may find necessary.

5. We acknowledge the right of the SOL to reject our Technical Bid, without assigning any reason.

6. We declare that we have not been directly or indirectly or through an agent engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice for this work.

7. We understand that SOL may cancel the bidding process at any time and that SOL is neither bound to accept any Technical Bid, without incurring any liability to the bidders.

8. We agree and undertake to abide by all the terms and conditions of the Tender Document, including the Conditions of Contract.

In witness thereof, we submit this Technical Bid under and in accordance with the terms of the Tender Document.

Yours faithfully,

Date: (Signature, name and designation of the Authorized Signatory)

Place: Name and seal of the bidder

Appendix A-1

ANNEX-I

Details of Applicant

1. (a) Name:

   (b) Address:

2. Details of individual(s) who will serve as the point of contact/ communication with the SOL:

   (a) Name:

   (b) Designation:

   (c) Telephone Number:

   (d) Mobile Number:

   (e) E-Mail Address:

3. Particulars of the Authorized Signatory of the Applicant:

   (a) Name:

   (b) Designation:

   (c) Address:

   (d) Phone Number (office) ---------- Mobile: ----------

   (e) E-Mail Address:

APPENDIX – A-2

(On letter head of the bidder)

Letter comprising the Financial Bid

Dated:

To,
Officer on Special Duty,
5-Cavalry Lane,
University of Delhi,
Delhi-110007

Sub: Financial Bid for Selection of Managed Service Provider (MSP) for implementation of cloud services School of Open Learning

Dear Sir,

With reference to your Tender Document dated---------- we, having examined the document and understood its contents, hereby submit our Financial Bid for the aforesaid work. The bid is unconditional and unqualified

2. I/ We acknowledge that the School of Open Learning (SOL) will be relying on the information provided in the Financial Bid and the documents accompanying it, and we certify that all information provided in the Bid are true and correct; nothing has been omitted which renders such information misleading; and all documents accompanying the Bid are true copies of their respective originals.
3. The bid price/rate has been quoted by us after taking into consideration all the terms and conditions stated in the Tender Document and our own estimates of costs.
4. The prices of all items stated in the Financial Bid are firm during the entire period of contract. Any increase in process during the period of contract shall be to the Bidder's account. In case of reduction in the process, SOL shall take the benefit of reduction from the date of reduction in prices
5. We acknowledge the right of the SOL to reject our Bid without assigning any reason.
6. In the event of we are being offered to accept the rates determined by SOL as the approved rates payable for printing, we agree to consider the rates, and if found acceptable, to enter into an agreement in accordance with the contract that has been provided in the Tender Document. We agree not to seek any changes in the aforesaid contract and agree to abide by the same.
7. We shall keep this offer valid for 120 (one hundred and twenty) days from the BID Due Date specified in the tender document

8. I/ We hereby submit our Bid and offer the rates for different items of work as per Annex I attached.

Yours faithfully,

Date:

Place:

(Signature, name and designation of the Authorized Signatory)
Name & seal of Bidder/Lead Member: ----------
Class III DSC ID of Authorized Signatory: ----------

APPENDIX – A-2 **Annex-I**

FINANCIAL BID

Sl. No.	Items (with minimum specifications)	QTY		Unit Price (INR)	Total Amount (INR)
	Option – A with DB-Oracle				
1	VM - 8vCPUs, 16 GB RAM Windows	4	Hours		
2	VM – 2vCPUs, 8 GB RAM VPN Server	1	Hours		
3	1 Hosted Zone (DNS)	1	Monthly		
4	SSD Storage 150 GB	1	Monthly		
5	Storage 10 TB	1	Monthly		
6	Data Transfer out (Per GB)	1	1GB		
7	Oracle Standard Edition 1 DB 8vCPUs, 16 GB RAM (20 GB database, Including Licensing Cost))	1	Monthly		
8	Managed Services (Implementation, Management and Maintenance of VMs & DB) (DB, OS Management) Backup Management	1	Monthly		
9	100 Mbps Lease Line 1:1 (site to site VPN to cloud with all devices, Except Installation Cost)	1	Yearly		
10	One Time Cost (Lease Line)				
11	CDN Cost	1	GB		
12	Machine Snapshot (Whenever Required	1	1GB		

13	Load Balancer	1	Hours		
14	Machine Image (Whenever Required)	1	1GB		
15	Live streaming per minute basis	1	Minute		
16	Live video packaging	1	Per GB		
17	Transcoding	1	Minute		
Option – B with DB-Postgre-latest version					
1	VM - 8vCPUs, 16 GB RAM Windows	4	Hours		
2	VM – 2vCPUs, 8 GB RAM VPN Server	1	Hours		
3	1 Hosted Zone (DNS)	1	Monthly		
4	SSD Storage 150 GB	1	Monthly		
5	Storage 10 TB	1	Monthly		
6	Data Transfer out (Per GB)	1	1GB		
7	Postgres DB 8vCPUs, 16 GB RAM (20 GB database, Including Licensing Cost))	1	Monthly		
8	Managed Services (Implementation, Management and Maintenance of VMs & DB) (DB, OS Management) Backup Management	1	Monthly		
9	100 Mbps Lease Line 1:1 (site to site VPN to cloud with all devices, Except Installation Cost)	1	Yearly		
10	One Time Cost (Lease Line)				
11	CDN Cost	1	GB		
12	Machine Snapshot (Whenever Required	1	1GB		

13	Load Balancer	1	Hours		
14	Machine Image (Whenever Required)	1	1GB		
15	Live streaming per minute basis	1	Minute		
16	Live video packaging	1	Per GB		
17	Transcoding		Minute		
	Total				

(SOL may award the contract on the basis of L1 either using Option – A-DB Oracle – B-Db Postgre. Even SOL will award the contract initially with Option – A for six months or till the migration to Postgre, i.e. Option – B after ward the rate of contract will change to Option – B).

Notes:

1. The above quantities are based on the current requirement assessment. If the requirement of any further application arises, the above quoted rates will be considered on proportionate basis as per the actual requirements.
2. All licenses cost should be included above quotes, as per requirement we can buy more licenses & Nodes as per above quotes
3. There will be no separate payment against installation or any other onetime charges for upgrading of oracle database along with restoring the existing backup.

Notes:

1. Any item/ material either hardware or software required to meet the functionality specified in the tender document whose related component is missing in the above table has to be accounted by the Bidder and the price of the same is assumed to be reflected and taken care in the price specified to the Client by the Bidder in this Financial bid. The Client is liable only to pay the Contract price as per the payment terms mentioned in the Tender Document to meet all the requirements as specified in the Tender Document.
2. All the rates will be calculated on a single unit of measurement.
3. Requirement is that the cloud provider should provide firewall as a service that would enable allowing or deny of network traffic.
4. Requirement is that the cloud provider should provide a layer 7 load balancer as a service so that applications are load balanced.
5. Block Storage/SSD Storage: Cloud provider should provide Managed SSD disk with minimum 3 IOPS / GB.
6. Managed Relational database service should support synchronous replication of a primary database to a standby database running copy in a separate physical data centre which are fault tolerant and completely isolated to each other to support redundancy and near zero downtime in case of a data centre facility failure.

7. Application should be setup in HA mode across multiple Data Centers which are fault tolerant and completely isolated to each other, connected through a low latency network to support redundancy and near zero downtime in case of a data centre facility failure.
8. Both Video-on-demand and Live Streaming - Media Service should have features which allows encoders to automatically determine the right number of bits to use for each part of video, basis the complexity of the scene, to maintain specified quality.
9. All VMs shall be on 2.3 GHz speed or higher.
10. CDN should be provided by CSP Only, Not in partnership/Collaboration with any third-party vender
11. Up time SLA 99.95, using high availability (2 unique data center which are fault tolerant each other).

12. CSP should provide and fully supported and maintained Open Source Cluster Management tools that makes it easy to deploy and manage high performance computing cluster in the Clouds. This tools provide support for Multiple SSD drive, Auto scaling, Batch Processing, Identity and Excess.
13. CSP should be provided Intel Sky lake processor & Above.
14. Live streaming – CSP should provide broadcast grade like video processing service which is highly available, automatically provisions the resources and its charges on a per minutes basis of usage. This should support the compression standard the use for video, like H.264/AVC and h.265/HEVC and media Communication protocols such as RTP, HLS/RTMP. Service should also provide support for captioning and multiple language audio tracks.
15. Live Video Packaging – CSP should provide live video packaging service which is highly available, Automatically provisions the resources and is charged on a per GB basis of usage.
16. Reread "The Cloud Service Provider - audited and approved by MeitY"
17. Load Balancing – CSP should provide Application and Network load balancing service which is highly available and is able to balance traffic to different instances placed in different fault tolerant data centers. Pricing of this service should be on the basis of actual usage defined in terms of hours of usage, New connections, Active connections, Processed bytes and no. of rules evaluated.
18. All services should be provided by a single CSP and not in partnership with any other provider except leased line.
19. The prices shall be inclusive of all taxes, rates & duties, except the GST, which shall be payable extra as per the prevailing rates.
20. The quantities mentioned are purely for the purpose of bid evaluation to reach at the L1 prices; these are bound to change as per the requirements.
21. The bidder will be evaluated based on the price quoted.
22. All the prices will be valid for 12 months. Any price increase at the end of year 1 will be notified separately to SOL. Any increase in prices during the period of contract shall be to the Bidder's account. In case of reduction in the prices, SOL shall take the benefit of reduction in price from the date of reduction in prices.

Bidders need to add their proposed specifications in case of any additional requirement

APPENDIX: B

Officer on Special Duty
School of Open Learning
5, Cavalry Line
University of Delhi
Delhi – 110007

Sub: Under-taking regarding Blacklisting/ Non-Debarment

Sir,

We hereby confirm and declare that we. M/s …… is not blacklisted/ Debarred by any govt. Deptt./ Public Sector Undertaking/ Private Sector or any other agency for which we have executed/ undertaken the works during the last 3 years.

For ……

Authorized Signatory with seal

APPENDIX -C

CERTIFICATE REGARDING TURN-OVER OF TENDERER DURING THE LAST THREE FINANCIAL YEARS

I / We, M/s _____, the Bidder/ Tenderer for **Selection of Managed Service Provider (MSP) for implementation of cloud services in School of Open Learning** hereby confirm that the minimum Annual Turn-Over of the firm/company during the last three financial years i.e. 2016-17, 2017-18 and 2018-19 is Rs 3 crore or more than Rs 3 (Three) crore.

The financial year-wise break-up is given below:-

FINANCIAL YEAR ANNUAL TURN-OVER FOR THE YEAR

S.No.	Year	Amount (In Rs.)
1	2016-17	
2	2017-18	
3	2018-19	

SIGNATURE & SEAL OF THE TENDERER

CERTIFICATE BY CHARTERED ACCOUNTANT

I / We, _____, Chartered Accountants, certify that the figures regarding Annual Turnover for the Financial Years mentioned above in respect of M/s. _____ are true and found correct as per their Books of Accounts and other related records.

SIGNATURE & SEAL OF THE CHARTERED ACCOUNTANT

SIGNATUR

APPENDIX: D

TENDER ACCEPTANCE LETTER

(To be given on Company Letter Head)

To
Officer on Special Duty
School of Open Learning,
5 Cavalry Line
University of Delhi,
Delhi-110007

Sub: Acceptance of Terms & Conditions of Tender.

Name of Tender: - **“** **”** in the School of Open Learning, University of Delhi, Delhi-110007.

Dear Sir,

1. I/ We have downloaded / obtained the tender document(s) for the above mentioned 'Tender' for the web site(s) namely:
   “……. “in the School of Open Learning, University of Delhi, Delhi-110007" as per your advertisement, given in the above mentioned website(s).
2. l/We hereby certify that I/we have read the entire terms and conditions of the tender documents from Page No. _ _ to _ _ (including all documents like annexure(s), schedule(s), etc.,) and [/we shall abide hereby by the terms / conditions /clauses contained therein.
3. The corrigendum(s) issued from time to time by your organization too have all been taken into consideration, while submitting this acceptance letter.
4. I/We hereby unconditionally accept the tender conditions of above mentioned tender document(s) / corrigendum(s) in it’s totally / entirely.
5. In case any provisions of this tender are found violated, then SOL organization shall without prejudice to any other right or remedy be at liberty to reject this tender/bid including the forfeiture of the full said earnest money deposit also.

Yours faithfully,

Signature of the Tenderer with Official Seal

APPENDIX-E

Form of Bank Guarantee for Performance Security

In consideration of Officer on Special Duty, School of Open Learning, University of Delhi (hereinafter called "The SOL") having offered to award the work **for implementation of cloud services in School of Open Learning to** _____ Managed Service Provider (hereinafter called "the MSP") provided the MSP submits an irrevocable Bank Guarantee for Rs. ……. (Rupees…… only) as Performance Security for the work **for implementation of cloud services in School of Open Learning**

1. We, …… (hereinafter referred to as "the Bank") hereby undertake to pay to the SOL an amount not exceeding Rs. …… (Rupees……. Only) on demand by the SOL.
2. We, …….(indicate the name of the Bank) do hereby undertake to pay the amounts due and payable under this guarantee without any demure, merely on a demand from the SOL stating that the amount claimed as required to meet the recoveries due or likely to be due from the said MSP. Any such demand made on the bank shall be conclusive as regards the amount due and payable by the bank under this Guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs. …….. (Rupees …….only)
3. We, the said Bank further undertake to pay the SOL any money so demanded notwithstanding any dispute or disputes raised by the MSP in any suit or proceeding pending before any court or tribunal relating thereto, our liability under this present being absolute and unequivocal. The payment so made by us under this Bank Guarantee shall be a valid discharge of our liability for payment thereunder and the MSP shall have no claim against us for making such payment.
4. We, ……. (indicate the name of the Bank) further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said agreement and that it shall continue to be enforceable till all the dues of the SOL under or by virtue of the said agreement have been fully paid and its claims satisfied or discharged.
5. We, ……. (indicate the name of the Bank) further agree with the SOL that the SOL shall have the fullest liberty without our consent and without affecting in any manner our obligation hereunder to vary any of the terms and conditions of the said agreement or to extend time of performance by the said MSP from time to time or to postpone for any time or from time to time any of the powers exercisable by the SOL against the said MSP and to forbear or enforce any of the terms and conditions relating to the said agreement and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said MSP or for any forbearance, act of omission on the part of the SOL or any indulgence by the SOL to the said MSP or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.
6. This guarantee will not be discharged due to the change in the constitution of the Bank or the MSP.
7. We, ……. (indicate the name of the Bank) lastly undertake not to revoke this guarantee except with the previous consent of the SOL.

8. This guarantee shall be valid up to ……unless extended on demand by the SOL. Notwithstanding anything mentioned above, our liability against this guarantee is restricted to Rs. …… (Rupees ……..) and unless a claim in writing is lodged with us within six months of the date of expiry or the extended date of expiry of this guarantee all our liabilities under this guarantee shall stand discharged. Dated the ……..day of ……for…….(indicate the name of the Bank)

APPENDIX - F
CONTRACT AGREEMENT

Format of the Agreement between SOL and bidder

INDIAN NON-JUDICIAL STAMP PAPER

Government of National Capital Territory of Delhi

e-Stamp

CONTRACT AGREEMENT

THIS AGREEMENT made on the -------- day of ----------, 2017 between School of Open Learning (SOL), University of Delhi, Delhi-110007 (hereinafter called **"SOL")** of the one part and (Name of bidder) M/s.---------- Address ---------- (hereinafter called **" Contractor "**) of the other part.

1. Whereas SOL has awarded the Tender for selection of Managed Service Provider (MSP) for implementation of Cloud Services in **School of Open Learning** based on his Technical and Financial Bid and whereas the bidder has accepted the schedule of Approved Rates offered by the SOL to the Contractor.

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

2. In this agreement words and expressions shall have the same meaning as are respectively assigned to them in the Conditions of Contract referred to.

3. The Contract Agreement consists of the following documents which are the part of Tender Document for Tender for selection of Managed Service Provider (MSP) for implementation of Cloud Services in **School of Open Learning.**

S. No.	Description of contents	Section
1	e- Tender Notice	
2	Introduction	I
3	Scope of work	II
4	Instruction to bidders	III
5	Commercial conditions	IV
6	Service Level Targets	V
7	Check List	VI
8	Technical Bid	Appendix A-I
9	Financial Bid	Appendix A-2
10	Undertaking regarding Blacklisting	Appendix-B
11	Performa for Annual Turnover	Appendix - C
12	Tender acceptance letter	Appendix - D
13	Form of performance bank Guarantee	Appendix- E

4. In consideration of the payments to be made by the SOL to the bidder as hereinafter mentioned, the contractor hereby covenants with the SOL to provide the services and to remedy defects therein in conformity in all respects with the provisions of the Tender Document including this Contract.

5. The SOL hereby covenants to pay the contractor in consideration of the provision of the services and the remedying of defects therein, the schedule of Approved Rates as finalized by the SOL and accepted by the contractor and such other sum as may become payable under the provision of the contract agreement applicable at the time and in the manner prescribed by the Conditions of Contract.

6. GST (Goods and Services Tax) where applicable will be reimbursed if claimed.

Authorized Signatory of the Firm

Officer on Special Duty
School of Open Learning,
University of Delhi, Delhi-110007