NATIONAL CENTRE FOR EARTH SCIENCE STUDIES
(An Institution under the Ministry of Earth Sciences, Govt. of India)
P.B. No. 7250, Akkulam, Thiruvananthapuram-695 011, Kerala.
PURCHASE DIVISION

Our Ref : PUR-PROC/73/2024-PUR-NCESS **Dt. 08/07/2024**
(To be quoted in all correspondence)

Phone :(0471) 2511531
FAX: (0471) 2442280
E-mail: purchase.ncess@nic.in
ncesspurchase@gmail.com
website : ncess.gov.in

CORRIGENDUM No.2

Tender No. PUR-PROC/73/2024-PUR-NCESS
For Upgradation of NCESS Data Centre Servers, Storage, SAN Switches and Virtualization Software along with Asset/Patch Management and EPM solutions

Change in tender specifications and conditions

Change in tender clause		
Sl. No	**For**	**Read**
1	Preference to Make In India: Preference will be given to the eligible Make in India offered products, in accordance with the CVC letter No. 018/VGL/022-377353 dated 20.04.2018, pertaining to Department of Industrial Policy and Promotion (DIPP) in connection with Preference to Make in India, Order 2017'(PPP-MIIOrder) dated15.07.2017 pursuant to rule153(iii) of General Financial Rules 2017. (Declaration may be submitted).	Modification to Clause 5 under Instructions to the Tenderers and Terms & Conditions - As per the approval of the Competent Authority, this tender is exempted from MII Clause

Modification to the Specification as decided in the prebid by the Committee have been highlighted. All the other terms and conditions remain unchanged :-

Scope of Work:-

*Upgradation of Existing 3 tier Server Storage Architecture to HCI solution with Minimum 3 nodes.

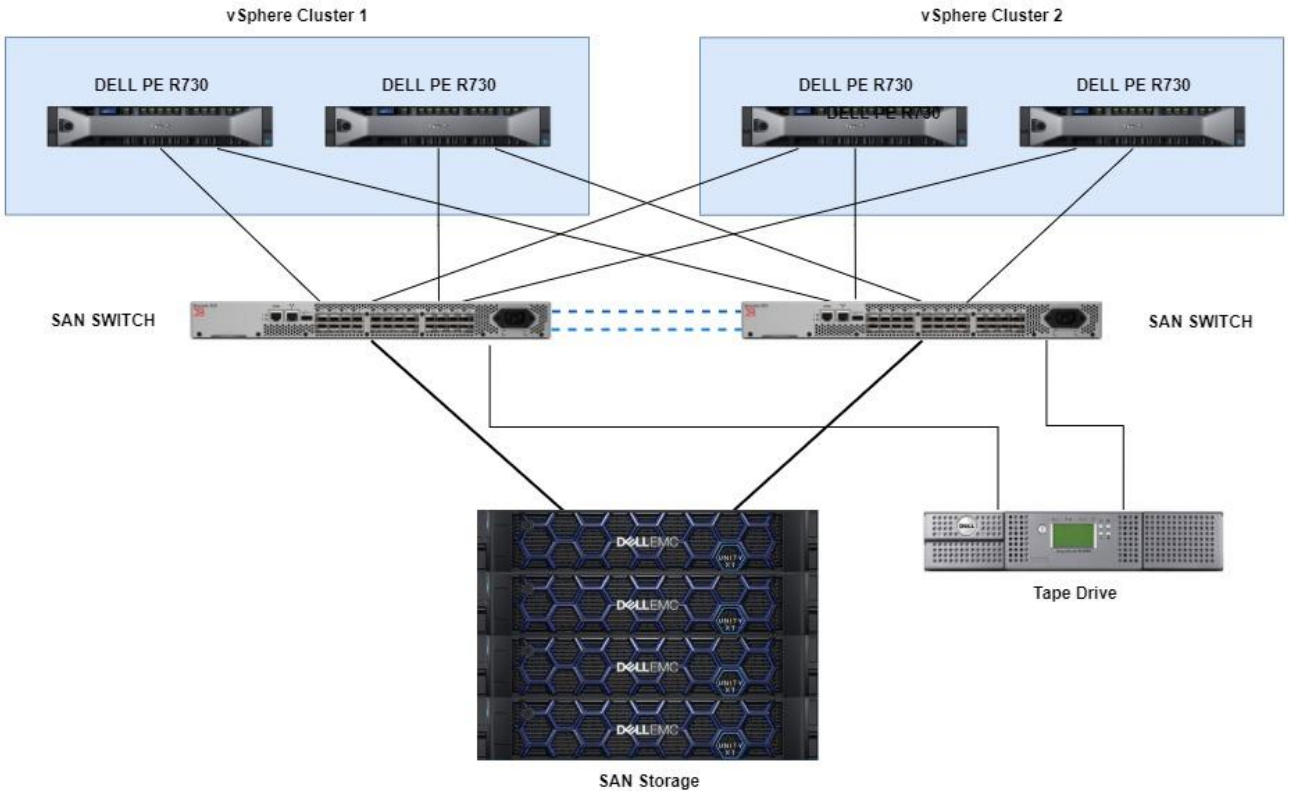
* Migration of all Existing Virtual solution from Vcentre 6, V sphere 6 and VM 24Nos Aprox-(Windows and Linux) to the HCI solution with Zero Down time.

* Migration of all running services on the existing Storage including NAS shares (8Nos Aprox with 40TB's of Data), FTP services, other Offline Data storage etc. to the HCI solution with Zero Down time.

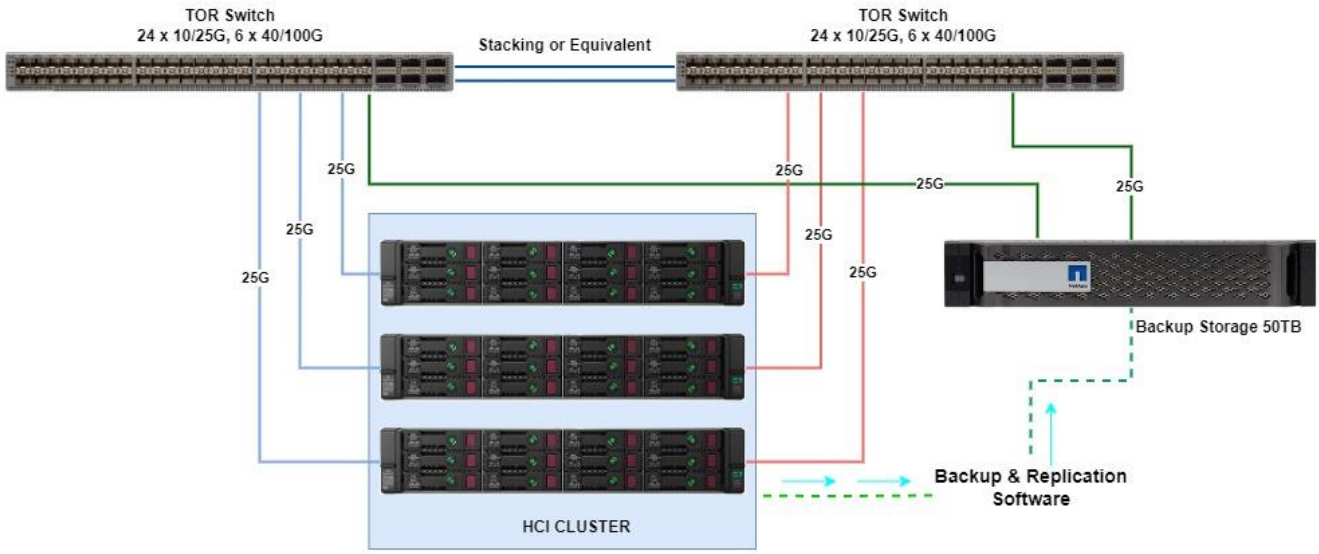
* Supply and Implementation of Asset manegement- Patch Management and EPM(EndPoint Privilege Management) Solutions- As Part of the Cyber Security Implementation acivities in NCESS.

* Following project commissioning, the bidder/supplier should provide technical documentation and training to NCESS technical personnel.

Existing Infrastructure:-



Proposed Infrastructure: -



Required Items and Description/Unpriced BOM: -

Sl No	Item & Description	Qty	Modifications
1	Supply, installation and commissioning of Hyperconverged Infrastructure 3 Nodes with 5 years onsite warranty and support with all necessary Virtualisation Licenses.	1	Supply, installation and commissioning of Hyperconverged Infrastructure consisting of Minimum 3 Nodes with 5 years onsite warranty and support with all necessary Virtualisation Licenses.
2	Top Of the Rack Switch (HCI Switch) 24 x 10/25G Ports, 6 x 40/100G Ports with 5 years onsite warranty and support.	2	Top Of the Rack Switch (HCI Switch) 24 x 10/25G Ports, 4 x 40/100G Ports with 5 years onsite warranty and support.
3	Backup Storage - 50 TB Usable Capacity (RAID level 6 or equivalent/higher) with 5 years onsite warranty and support.	1	Backup Storage - 100 TB Usable Capacity (RAID level 6 or equivalent /higher) with 5 years onsite warranty and support.
4	Backup software (Perpetual) for 25 VMs, 30TB Storage, with 1 year support from OEM.	1	Backup software (Perpetual) for 30 VMs, 50TB Storage, with 5 year support from OEM.
5	Microsoft Windows Server 2022 Datacenter (for 72 Cores with unlimited VM support)	1	Microsoft Windows Server 2022 Datacenter or higher (for total Cores quoted with unlimited VM support)
6	Supply and Implementation of Asset manegement- Patch Management Solutions for 250 Endpoints with 5years support.	1	
7	Supply and Implementation of EPM(EndPoint Privilege Management) Solution for 250 Endpoints with 5years support.	1	

Detailed Technical Specification: -

	Hyper Converged Infrastructure - 3 Nodes	**Hyper Converged Infrastructure – Minimum 3 Nodes**
Sl No	**Technical Specification**	
1	The proposed solution should be Hyper-Converged Infrastructure appliance that come pre-installed with various software including Software Defined Storage with Enterprise class Storage Services, replication with management and associated hypervisor.	
2	The solution shall provide hyper-converged infrastructure that allows delivery of enterprise-class storage services using latest x86 server infrastructures without dependence on a separate Storage Area Network associated component such as SAN Switches and HBAs.	
3	HCI solution should be based on modular scalable architecture having the ability to add and auto-discoverable nodes. It must support automated cluster deployment using templates, configuration, and non-disruptive updates.	
4	**HCI Configuration:**	
	The solution should provide 100TB usable capacity across three (3) nodes with **N+1 failover plan.**	The solution should provide 30TB usable capacity across all nodes with (each node size 1U or higher) **N+1 failover plan.** 30TB of usable storage should be available even after one node failure.

	Each node should have 2x12 core intel Xeon Gold/Silver Processors (2.1 GHz or higher)	Each node should have Intel Xeon Gold/Silver Processors (2 GHz or higher). The solution should provide 72 usable cores across the cluster. Any HCI CPU overheads should be considered extra.
	Each node should have minimum 256GB 3200MHz DDR4 Memory	Total solution should have Minimum 768 Usable memory (3200MHz DDR4) across the cluster. Any HCI memory overheads should be considered extra.
	Each node should have minimum 2nos of dual port 10/25G SFP28 NIC cards	Each node should have Minimum 2nos of dual port 10/25G SFP28 NIC cards. Populated with 10G multimode Transceivers.
	The usable storage should be calculated with RF2/RAID10.	The usable storage should be calculated considering RF2/FTT1 /RAID5/ RAID10.
	Minimum 10% of usable storage should be on SSD	The proposed solution should be All-Flash
	Space Efficiency features (de-duplication or compression) should not be considered for usable storage calculation.	
5	The solution should have provision for Cryptographic firmware updates, Capability to stop execution of Application/Hypervisor/ Operating System on predefined security breach, Secure /Automatic BIOS recovery, Network Card secure firmware boot, in case of any security breach system should provide the lock down feature.	
6	Secure Boot (Firmware and Bios Level Security), Provision to lock the system on breach, Hardware root of trust/Dual Root of Trust, Server should provide policy-based security, Server should provide server intrusion detection, "Malicious Code Free design" (to be certified by OEM)	
7	Proposed HCI should support standard features like VMotion or equivalent, affinity rules, automated/dynamic resource scheduling and replication. Demonstration of this shall be given after bid opening, if asked.	
8	The solution should provide enterprise data services such as de-duplication and compression without dependence on any proprietary hardware.	The solution should provide enterprise data services such as de-duplication and compression.
9	Virtualization software shall provide a virtualization layer that sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability and security.	Virtualization software shall provide a virtualization layer that sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability and security. Also, the virtualization software must include USB pass-through capabilities to facilitate access to USB dongle/token licenses on the VMs. If the feature is not part of the Hypervisor, the bidder should consider and provide the third-party rack-mountable USB over IP Hub for at least connecting a minimum of 10 ports with comprehensive warranty, necessary subscription or support for five years.
10	The proposed HCI solution should be proposed with enterprise grade hypervisor like AHV/Hyper-V/vSphere.	

11	Proposed HCI shall support to, hot-add CPU & Memory without the need to reboot the VMs (if the underlying guest OS supports). All the features should be made available in GUI base interface for ease of operation.	
12	The solution should be capable of intelligent placement for workloads, so that the load gets distributed dynamically without manual intervention and get efficient performance.	
13	The solution should provide a virtual switch that can span across a virtual data enter and multiple hosts should be able to connect to it. This in turn will simplify and enhance virtual machine networking in virtualized environments.	
14	The solution should support data replication and application consistent snapshots. There should not be any limitation on number of VMs to be replicated.	
15	The solution should provide a single unified management console for the management of the entire environment including virtualized environment as well as software defined storage environment, underlying Hardware and associated components.	
16	HCI solution management pane should be integrated with Active Directory /LDAP.	
17	The proposed HCI must natively support scale-out File Services (NFS, CIFS & SMB) without use of 3rd party tools. The solution should be able to provide the detailed insights of the data stored in file storage based on the data age, size and data type. Required licenses to be supplied for 15TB of file storage from day 1.	The proposed HCI must support scale-out File Services (NFS, CIFS & SMB) with/without use of 3rd party tools.
18	HCI Solution with integrated file storage should be able to audit all users, for files AMD (Access/Move/Delete) operations with track for all type of access for data as per assigned rights.	This clause has been removed.
19	Virtualization software should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues.	
20	The proposed solution shall provide the ability to push updates and patches specific to the Virtualization and HCI Infrastructure without any impact to the VMs. During the upgradation activity the offered solution shall ensure that there is no data loss.	
21	The solution should support multi-tenancy and should have inbuilt NAT functionality so that overlapping IP addresses can be used across multiple tenants.	This clause has been removed.
22	The Proposed solution shall support future addition of nodes with different CPU models and memory capacity/configuration in the same cluster.	
23	The HCI solution should support hybrid & all-flash nodes in the same cluster. And shall support adding heterogeneous configuration nodes to the same cluster.	This clause has been removed.

24	HCI solution must support Kubernetes key automation for multi master/worker provisioning with storage Integration with require storage e.g. File/Block/Object with seamless upgrade rollout using automation engine.	
25	Must have provisioning, operations and lifecycle management of Kubernetes, automated deployment, scaling, and operation of application containers across a cluster of hosts.	
26	The solution quoted shall provide with storage/VM level snapshots for local backups or equivalent.	
27	The solution shall support integration with popular third-party data backup/protection solutions.	
28	The License supplied shall not limit the number of VMs.	
29	Proposed solution should have at least two or more industry certifications like NIST, FIPS140-2, EAL2 CCC-Common Criteria Certified, DISA- approved STIG.	
30	The OEM shall have a minimum of 100 node installations of the proposed HCI solution in the Government organizations in India.	The OEM should have a minimum 5nos of 3-node HCI installations during the last 3 years.
31	Shall include direct OEM, L1, L2 and L3 support for 5-years, 8x5xNBD for hardware(repair/replacement) and 24x7x365 days with unlimited incident support (Telephonic/ Web/ Email) and technical contacts within 60 mins or less response time including the unlimited upgrades and updates for software.	

	TOR Switches		
Sl No	**Specification**	**Description**	**Modifications**
1	Solution Requirement	The Switch should support non-blocking Layer 2 switching.	
		Switch should support the complete STACK of IPv4 and IPv6 services.	
		The proposed switches should be part of Gartner Leader Quadrant for DC Networking for last 3 years.	The proposed switches should be part of Gartner Leader Quadrant for DC Networking/Wired and Wireless LAN Infrastructure for last 3 years.
		Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN	
		Switch should support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre.	
		The Switch used have the capability to function in line rate for all ports.	
2	Hardware and Interface Requirement	Minimum 24 ports support 1/10/25 Gbps SFP ports for host connectivity and 6*40G/100G ports for Fabric/Spine connectivity. The proposed switch should support native 25G and should be populated with 24*10G Multimode fibre transceivers	Minimum 24 ports support 1/10/25 Gbps SFP ports for host connectivity and 4*40G/100G ports for Fabric/Spine connectivity. The proposed switch should support native 25G and

		for downlink connectivity & 6*40G/100G ports with multimode 100G Transceivers, for uplink connectivity.	should be populated with 24*10G Multimode fibre transceivers for downlink connectivity & 4*40G/100G ports with multimode 100G Transceivers, for uplink connectivity.
		Switch should have console port for local management & management interface for Out of band management.	
		1 RU fixed form factor.	
3	Performance Requirement	Switch should support minimum 1000 VRF instances with route leaking functionality.	Switch should support minimum **250 VRF** instances with route leaking functionality.
		The switch should support **400k** IPv4 LPM routes and Maximum number of VLANs supported is 4096.	The switch should support **130k** IPv4 LPM routes and Maximum number of VLANs supported is 4096.
		The Switch should support intelligent buffer management with a minimum buffer of **40MB**.	The Switch should support intelligent buffer management with a minimum buffer of **32MB**.
		Switch should support Maximum number of MAC address entries 512k.	Switch should support Maximum number of MAC address entries **90k**.
4	Layer2 features	Switch should support FCoE.	This clause has been removed.
		The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN).	
		Maximum number of port channels should be 24.	
		Maximum number of IP host entries supported should be 1,792,000 or more.	Min number of IP host entries supported should be 120K or more.
		The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane.	The switch should support BGP EVPN Route Type 2, Type 4 or equivalent, and Route Type 5 for the overlay control plane.
5	Layer3 features	Switch should support static and dynamic routing.	
		Switch should support segment routing and VRF route leaking functionality from day 1.	This clause has been removed.
		Switch should support Segment Routing and Layer3 VPN over Segment Routing.	This clause has been removed.
		Switch should support multi-instance routing using VRF/ VRF Edge/ Virtual Router routing and should support VRF Route leaking functionality.	
		Switch platform should support MAC Sec (802.1AE) encryption in hardware.	This clause has been removed.
6	Management	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces.	

		Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.	The switch OS should support programmability through REST APIs and Python scripting or equivalent.
		The Switch Should support monitor events and take corrective action like a script when the monitored events occur.	
		•Flow path trace (ingress to egress switch).	
		• Latency and packet drop.	This clause has been removed.
		Flow telemetry should support hardware acceleration so that it is not impacting CPU performance.	This clause has been removed.
7	Warranty & Support	5 Years warranty and support including transceivers should be provided with Next Business Day support. All the upgrades, updates and patches shall be provided within the support period.	

	Backup Storage		
Sl No	**Specification**	**Description**	**Modifications**
1	Storage Quality Certification	The Storage OEM should be established in the Gartner Leader Quadrant.	
2	Storage Controller	The Storage Solution should be based on dual controllers in active-active mode configured in a NSPOF offering data assurance as per T10-PI standard and End-to-End Data Protection.	The Storage Solution should be based on dual controllers in active-active mode.
3	Cache required	The system should have minimum 16GB cache memory across the two controllers with an ability to protect data on cache if there is a controller failure or power outage. The cache on the storage should have 72hrs or more battery backup (OR) should have destaging capability to either flash/disk and also offer extended cache based on SSD with the facility to allow changing of cache block size non-disruptively for defined RAID group levels to meet various kind of workload.	The system should have minimum 64GB cache memory across the two controllers with an ability to protect data on cache if there is a controller failure or power outage. The cache on the storage should have 72hrs or more battery backup (OR) should have destaging capability to either flash/disk and also offer extended cache based on SSD with the facility to allow changing of cache block size non-disruptively for defined RAID group levels to meet various kind of workload.
4	Drive Support	The system must support intermixing of SSD, SAS and NL-SAS/SATA drives to meet the capacity and performance requirements of the applications.	
5	Protocols	The storage should be configured with FCP & iSCSI protocols. Any hardware/software required for this functionality shall be supplied along with it in No Single Point of Failure mode.	The storage should be configured with either FCP or iSCSI protocols. Any hardware/software required for this functionality shall be supplied along with it in No Single Point of Failure mode. The storage should be Unified, and any NAS gateway system is not acceptable.

6	RAID configuration	Should support various RAID levels including RAID 6.	
7	Storage Capacity	Minimum 50TB usable (RAID level 6 or equivalent/higher) with NLSAS disks and scalable to 2PB of capacity within same storage in similar or higher configuration.	Minimum 100TB usable (RAID level 6 or equivalent/higher) with NLSAS disks and scalable to 2PB of capacity within same storage in similar or higher configuration.
8	Drive Support	The system must support intermixing of SSD, SAS and NL-SAS dual ported drives to meet the capacity and performance requirements of the applications. The system must support a minimum of a 180 disks per two controllers for scalability purpose and must use every drive, up the supported count of drives per pool, spreading out all volumes across all drives and also decrease the drive rebuild time.	The system must support intermixing of SSD, SAS and NL-SAS dual ported drives to meet the capacity and performance requirements of the applications. The system must support a minimum of a 140 disks per controller for scalability purpose and must use every drive, up the supported count of drives per pool, spreading out all volumes across all drives and also decrease the drive rebuild time.
9	Front-End and Backend connectivity	The proposed storage system should have minimum 4 numbers of 12Gbps or higher backend SAS ports, 4 numbers of 10Gb FC / SFP+ ports and Minimum 4 x 10/25G SFP28 Ports.	The proposed storage system should have Minimum 4 numbers of 12Gbps or higher backend SAS ports, Minimum 4 x 10/25G SFP28 Ports with 10G optics.
10	Rack Mountable	The storage should be supplied with rack mount kit. All the necessary patch cords (Ethernet and Fiber) shall be provided and installed by the vendor.	
11	Storage functionality and Availability	The storage shall have the ability to expand LUNS/Volumes on the storage online and instantly.	
		The storage shall have the ability to create logical volumes without physical capacity being available or in other words system should allow over-provisioning of the capacity. The license required for the same shall be supplied for the maximum supported capacity of the offered storage model.	
		The proposed storage system should be configured to provide data protection against two simultaneous drive failures.	
		The required number hard disks for parity & spares, should be provided exclusively of the usable capacity mentioned after consider RAID and Filesystem overhead. At least 2% of the usable capacity requested on each tier should be configured as spare drives with the subsequent disk types.	
		Storage system should support RAID level distributing data across multiple Disk to ensure faster rebuild time.	
		The offered system should support a REST API, open-source orchestration and compatibility of configuration management for easy integration and automation in traditional IT and Windows ecosystems.	

		System should have redundant hot swappable components like controllers, disks, power supplies, fans etc.	
		The proposed system should offer & support various security features such as encrypted drives (FDE/FIPS), internal and external encryption key management (KMIP-compliant), Role-based access control, audit log, LDAP support, Multi-Factor Authentication. Licenses Required if any must be supplied.	
		The proposed system should offer up to six 9's of availability.	
12	Point-in-times images	The storage should have the requisite licenses to create point-in-time snapshots. The storage should support minimum 512 snapshots. The license proposed should be for the complete supported capacity of the system.	
		The system should support instant creation of clones of active data.	
13	Management	Easy to use GUI based administration interface for configuration, storage management and performance analysis tools. The proposed storage should provide Proactive monitoring of the health of the system and configurable automated delivery of replacement drives when failures occur.	
14	OS support	Support for industry-leading Operating System platforms including LINUX, Microsoft Windows, HP-UX, SUN Solaris, IBM-AIX, etc. It shall support connecting hosts over iSCSI or FC and shall be supplied with any Multipathing software, if required, with the solution.	Support for industry-leading Operating System platforms including LINUX, Microsoft Windows etc. It shall support connecting hosts over iSCSI or FC and shall be supplied with any Multipathing software, if required, with the solution.
15	Warranty & Support	The Hardware and software quoted should have 5 years onsite support along with upgrade and updates.	

	Backup Software		
Sl No	**Specification**	**Description**	**Modifications**
1	Analyst Rating	Backup software proposed should be in Gartner's leader quadrant for last five years in Gartner Magic Quadrant report for Data Protection / Backup Software.	
2	Licensing	The proposed Backup software must offer host based or instance-based licenses with no restrictions on type of arrays (protecting heterogenous storage technologies) or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied for both primary and DR	

		site.	
		The proposed data protection solution should provide single license file to protect virtual machines, physical servers, NAS workload, Endpoints and multi cloud workload including all database applications running on these platforms	
		The proposed backup software should have a native solution to protect Kubernetes/Container workloads; without the need of a 3rd party solution.	
3	Reporting Capabilities	Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.	
4	Data Protection and Recovery in the cloud	Software should be able to restore VMs to a cloud service provider like AWS, Azure, Google or any private cloud vendor directly from the backup copy.	
		Software should be able to extend the backup repository to a public/private cloud service provider by moving older files to any S3 Compatible Object storage or Azure BLOB repositories.	
		Backup software should have capability to archive data to Amazon Glacier or Microsoft Azure storage Archive Tier. The Software must have capability to restore the data from archive tier, it should not be dependent on cloud vendor.	
		Backup software should support agentless backups of applications residing in VMs like SQL, Exchange, Share-point, Oracle, etc. with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads. Backup software should support SAP HANA backup integrated with HANA Cockpit.	
		The software must have the functionality to back up on-prem data directly into cloud repositories such as AWS S3 or Microsoft Azure Blob or any S3 compatible object storage.	

		Proposed backup software should be able to leverage Immutable Cloud based storage like S3-Immutable service to prevent backup copies of data from any corruption or ransomware attacks.	
5	Backup support for hypervisors and Applications	Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV and RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) as well for long term retention.	
		The proposed backup software should provide Instant recoveries for any backup to VMware, Hyper-V or AHV Virtual machine.	
		Backup software should support file level recovery from any backup of any VM or physical server. It should support a full system recovery in case of a system crash, either on a physical system or virtual machine or as a Cloud Instance (AWS, Azure or Google).	
		Backup software should have integrated data de-duplication engine with multi-vendor storage support to save space by storing de-duplicated copies of data. The de-duplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components.	
		Backup software should support instant database recoveries of MS SQL and Oracle from the backup files.	
		Backup software should support Multi factor authentication for accessing Backup console and console auto log-off functionality.	
6	RPO/ RTO and Recovery Assurance	Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability.	
		Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest	

		OS and Application Consistency and then publish automated reports to be used in backup / recovery audits.	
		Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only of those VMs to which they have access, without administrator intervention, thereby delivering self-serve capabilities.	
		Proposed backup software should be able to Harden the repository on any Linux platform. This service will prevent backup copies of data from any corruption or ransomware attacks.	
		The software should support Group Managed Service Accounts which should have an option for users to allow change passwords after every 30 days and adapt complex password policy.	
		The proposed backup software should be able to integrate with anti-virus software and scan before recovery of VMs and ensure that any infected VM is not restored or restore it with disabled network adapters to prevent any infection to spread through the network.	
		Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be restored from the backup copies. This will help in complying to "right to be forgotten" regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.	
		Backup software should support instant file share recovery in NAS storages to allow users to access files fast after disaster.	
7	Backup and Replication Performance and SLA	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads.	

		Backup software should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup within 15Mins RTO.	
		The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.	
8	Disaster Recovery Capabilities	Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also include failover and failback capabilities and should be able to perform automatic acquisition of network addresses at the destination site.	
		The Proposed solution should support Continuous replication at VM level. The RPO must be less than 5 Seconds and it must deliver Application consistency.	
		Backup and replication software must deliver maximum investment protection by supporting replication of workloads between dis-similar systems like hyperconverged infrastructure to stand alone servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production workloads irrespective of the underlying hardware.	
		Backup software should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes. This bare metal recovery capability should be built in for the physical servers and should even work on the dissimilar hardware.	
		Backup software should have the ability to backing up a Cloud VM running in AWS or Azure and restore it as a valid VM workload back onto a VMware server farm.	

9	Required Quantity	The license should be provided for the backup of 25 VMs (Both Windows and Linux based), and 30TB of storage volumes	
10	Support/Subscription	The license should be perpetual with minimum 1 year support directly from OEM.	The license should be perpetual with minimum 5 year support directly from OEM.

Sl No	Description
1	**Patch management**
2	Proposed Patch Management solution should have the ability to do centralized patch management for PCs, Laptops, and Servers.
3	Proposed Solution Should Provide option to Schedule periodic scans of computers to identify missing patches.
4	Proposed Solution should support Windows, Linux and MAC OS patches.
5	Solution should download required patches only and based on created schedules, patch must be deployed on identified machines.
6	Solution must be supported for deployment of patches at endpoints and servers having Low bandwidth under a single management console.
7	Proposed Patch Management Solution should Schedule, deliver and track operating system patches to perform patch delivery based on its schedule.
8	Proposed Patch Management Solution should support centralized architecture.
9	Proposed solution should support local distribution points through preferred servers, should fallback to Central Server in case preferred server is down.
10	Easy-to-use configuration options for scheduling replication to reduce complexity and time in managing remote sites.
11	Solution should Use MD5 checksums and validation while doing any package or file transmissions between central server and distribution locations.
12	The Proposed solution should support before downloading the Patch signature need to verify the security checks.
13	The Proposed solution should Verify the patch metadata produced by each content.
14	The Proposed solution should Validate the patch installation and uninstallation processes.
15	The Proposed solution should Confirm that the patch does not disrupt the stability of the targeted operating systems and applications.
16	The suppress-reboot functionality works.
17	The uninstallation functionality works.
18	The proposed Solution should support automated patch management for critical security patch deployment on physical machines and other infra including Windows, Linux and Mac.
19	The proposed solution should support patch evaluation in a test environment before distributing.
20	The proposed solution should support rollback of patches applied on the machines.
21	The proposed solution should support remote patch management.
22	The proposed solution should come along with standard reports and can generate the customized reports as per business requirement. The Patch Management solution should be capable of generating real-time reports on patches deployed, when, by whom, to which endpoints, etc.
23	The proposed solution should provide mechanism to centrally set/reset registry value in target Window machine.
24	The proposed solution should be able to provide the package/software deployment as option to centrally deploy in target window machines.

25	The proposed solution should have an option to define multiple deployment policies for deploying patches.
26	The proposed solution should show the system health based on missing patches.
27	The proposed solution should have a customisable dashboard for viewing information like vulnerable systems, missing patches, deployed patches, etc.
28	The proposed solution should have capability to apply patches based on group/location.
29	The proposed solution should send notification over email and on screen upon patch failed/successful.
30	The proposed solution should support distributed relay/file server to optimize bandwidth utilization for patch download in distributed architecture.
31	The proposed Solution should support automated patch management for critical patch deployment on Windows endpoints/servers.
32	The proposed solution should support patch evaluation in a test environment before distributing.
33	The proposed solution should highlight missing critical patches and should re-attempt failed patches.
34	The proposed solution should support mechanism to decline or delay an unnecessary patch that may cause any problem to overall IT infrastructure.
35	The proposed solution should support rollback of patches and service pack applied on the machines.
36	The proposed solution should have an option to upload patches manually as well as get automatic patches from central repository.
37	The proposed solution should allow to specify the bandwidth limit for patch download.
38	The OEM of the proposed solution should have achieved ITIL certification on at least 6 available ITIL processes (a documentary proof of the same should be provided at the time of bidding).
39	The OEM of the proposed solution must be featured in Gartner/IDC reports. Documentary proof must be submitted at the time of submission.
40	The proposed OEM should possess Quality Management, IT Management security and Application Security Management certifications like ISO 9001, ISO 27001 and ISO 27034.
41	The proposed solution should have 24x7 OEM support.
42	The OEM of the proposed should be a company with presence of min. 10 years in the market.
43	The proposed OEM of proposed tool must have VAPT security certificate from cert-in empanelled organizations to meet security compliance.
44	The proposed patch management and asset management should be tightly integrated and should be from same OEM.
	Asset Management
1	The Proposed IT Patch and Asset Management (ITAM) Solution must provide the functionality of the current application and be compliant with Information Technology Infrastructure Library (ITIL) for ITSM. For ITAM, the Proposed Solution should cover several Key Process Areas of ITAM's Best Practice Library. The Proposed Solution must also provide tight integration between the patch management and ITAM processes.
2	The Information Technology Asset Management Solution shall be defined as scalable Web based solution with integrated Configuration Management Database which shall be responsible for management of all IT Assets.
3	Management of the IT Assets shall include the following: - Asset Discovery, Asset On-boarding, Asset Tagging, Asset Inventory, License Management, Life Cycle Management, Reporting Services.

4	Solution should be able to identify the IT Assets inside the network through Agent Based and Agent Less discovery techniques for IT assets through SNMP, ICMP, SSH, WMI etc for on premise devices as well as cloud infrastructure. It should support domain scan discovery as well to gather information such as: Information on the number and type of Hardware components (Processors/Core/USB/Network Card/USB etc.), Drivers/ Firmware, Graphics and Audio, Hard Drives, Hosted Virtual Machines, Logical Volumes, Memory, Network Interfaces, Operating System Updates Applied, Out of Band Management, Peripherals, Ports and USB Controllers, Processors , Removable Media, Software Inventory, Storage Controller, System Information, OS Update Information. · Make & Model of Hardware Components (Asset/Motherboard/RAM/Hard disk etc.) · Serial Nos of Hardware Components (Motherboard/RAM/Hard disk etc.) · Versions/Manufacture Dates of the Components · BIOS Details/ OS & Service Pack/Build/Version Details · IP/MAC Addresses · Peripheral Devices connected to the Assets. · Software Discovery – Applications (including Virtualised) / Software/ Patches etc.
5	The proposed Asset Management solution should have the capability of deployment through SaaS-based Asset Management, built on a common platform for unified enterprise service management.
6	The proposed Asset Management solution should can be deployed anywhere on the following deployment platforms: On- premises, Cloud, SAAS on Azure, AWS, etc.
7	The solution shall provide for life cycle management for both hardware and software assets. The solution shall track the life cycle through Purchase, In production, Renewals, End of Life and Disposal stages of the IT Assets.
8	Deployment & Discovery - Agent & Agent-less deployments, discover the assets in the network for software and hardware inventory, allocate software to a hardware asset, add relationship maps etc.
9	Maintain - Schedule scans and get audit history, Complete ownership tracking, Software compliance and license management, Asset depreciation calculations, Total cost of ownership of an asset, etc.
10	The solution should be deployable on Linux operating systems to reduce the overall TCO.
11	The solution should support tagging of assets with Barcode as well as QR code.
12	The Solution should be capable to support each local admin to maintain cost & depreciation sheets with respect to each asset / at Aggregate level within ASSET Management Tool itself.
13	The Solution should be capable to Integrate with AD / E mail / SMS Gateways.
14	Asset Management - All the assets in the network are broadly categorized. Etc.
15	Product and vendor - create Product Types and list various products under this, add the vendor details for a particular product such as vendor name, warranty period, price and much more. Etc.
16	Group assets and manage them - manage the assets and add the context, Static grouping, Dynamic grouping, and new resource to be automatically placed in the respective group.
17	View software compliance - keep track of all your software assets and licenses, group the software through various categories such as Software Type, License Type, vendor name etc.
18	Relationship between your business-critical resources - Ability to configure and monitor the various relationships of every business-critical asset in your network.
19	Software and Hardware inventory tracking - Track all IT assets - software and hardware, hardware to be identified are servers, workstations, printers, routers, switches & any devices with an IP address and connected to the network, OS - Windows, Linux, Solaris, Mac, VMWare ESX/ESXi etc.

20	Scan, Discover & Update - automatically scans the network, discovers IT assets (hardware and software) and updates whenever there is a change in any of IT assets.
21	Tracking Ownership, Status & Total Cost of Assets - accurately maintain a history of the asset that includes ownership history and changes during the asset's lifecycle, support and maintenance costs incurred by the asset helps you understand the real cost of the asset - Total Cost of Ownership.
22	Manage Contracts and License Agreements - gives details on the contracts, software licenses and vendors associated with that particular asset.
23	The proposed Asset Management solution should be able to track the location change movement of asset.
24	Manual Onboarding: For IT and Non-IT Assets not connected to the network, Solution shall allow for manual onboarding of the Assets. Manual onboarding shall be done through either or through a combination of the below: ➢ Upload of Asset data files (excel/word) into the solution.
25	Purchase Order Management - Create POs and define approver, Approve /Reject PO, Closed PO / Receive Asset.
26	Able to create a purchase order for an asset, component, or bulk item.
27	Asset records are automatically created when the items have been received or partially received if you have submitted a purchase order or a purchase requisition from a third-party procurement application that your application administrator has integrated with the Asset Management application.
28	Provide configuration catalogue for approved items for procurements purpose.
29	Contract Management - Create Contracts and associate any asset, Manage Contracts with Timely Alerts, Attach Term and Conditions.
30	Able to store contract data related to support contracts, warranties, leases, maintenance contracts, and software contracts and licenses for the organization's assets and components.
31	Able to create and view reminders associated with any of the contract form.
32	Able to store support contract terms for assets and components, include links to supplier information, enable the appropriate group or individual to be notified upon expiration of the support contract, and store and track payment information.
33	- Able to associate contracts info with assets and components.
34	CMDB - stores information on all the significant entities in your IT environment, the entities, termed as Configuration Items (CIs) can be hardware, the installed software applications, documents, business services and also the people that are part of your IT system.
35	Configuration Item Types - CI Type to be represented with Attributes and Relationships that is unique for the CIs classified under it, CI Type may form a hierarchical structure by further drilling down to Sub Types.
36	Access to computers on LAN and WAN for maintenance purpose Remote Access tool enabling access from anywhere in the LAN.
37	Ability to remotely do chat, voice call, video call, transfer files across machines.
38	Options for recording and viewing the recorded remote sessions to monitor the session activities, ensuring data security.
39	Web based remote control - provides a web-based connection to the remote computers.
40	User privacy protection – ability for administrators to opt for user's permission before connecting to their desktop.
41	Should manage all types of software license and hence software compliance.
42	Should be able to recover software licenses when hardware is retired, returned (for leases).
43	Should track version, status, and upgrade information for each installed software package.
44	The tool must be able to reconcile the number of Installed copies of an application with the number of permitted licenses.
45	Must include Reporting Services: -
46	The Solution should have ability to create multiple reports within the dashboard to map to security requirements and environment.

47	The Access to reporting function should be controlled based on rights assigned by the Master Administrator.
48	The Solution should allow console operators to create and save graphical reports (e.g. pie, bar, line charts).
49	The Solution should allow console operators to customize and save the reports without the use of third-party reporting tools.
50	The OEM must be an industry standard solution for Network Automation and Orchestration Tools report. Documentary proof must be submitted at the time of submission.
51	The proposed solution should come as a bundled solution along with database to reduce overall TCO.
52	The OEM of the proposed solution should be a company with presence of min. 10 years in the market. The documentary proof should be submitted at time of the bid submission.
53	OEM must have average annual turnover of at least INR 20 Cr. or above in last 3 financial years Excluding the current financial year with positive net worth. CA Certificate need to be submitted at time of bid submission.
54	The OEM of the proposed solution should possess Quality certifications ISO 9001, Information security certificate ISO 27001, Application security certificate ISO 27034 and CIS benchmark certificate. Documentary proof must be provided at the time of submission
55	The support should be provided for the one-time implementation and 5 years post implementation directly from OEM.

Sl No	**Endpoint Privilege Management**
1	The Proposed Solution should support Windows/ Linux / Mac OS as part of the Proposed Solution approach.
2	The Proposed Solution should give the power to monitor threats and behavioural changes present within users and entities (endpoints, applications, processes). It also serves as a global operations management product that provides visibility into your organization's operations on a real-time basis. This is achieved through the help of an agent which is installed on the end user machine which ensures even if user is not part of a domain is still under the restrictions and rules set by the organization's policy.
3	The Proposed Solution should also help in vaulting local admin passwords along with PAM.
4	The Proposed Solution should give the organization the flexibility to create policy to ensures users have access to only applications / process / commands until explicitly granted. These policies can be assigned to a particular user or group of users based on their roles.
5	The Proposed Solutions Intelligent Rules Engine can be used to enforce data protection and access control rules on the compromised user to prevent data exfiltration and other malicious attempts.
6	The Proposed Solution should come with multiple reports which organizations can use for analysis. Example Data visualization reports such as Sunburst graphs illustrate the use of processes by the user. It captures the duration of time spent on processes. It has sliced components, and each slice displays the duration in time spent on particular processes. A built-in drill down gives the ability to click and focus on one item at runtime and drill down into its details which helps more complex data analysis.
7	The Proposed Solution Should Let user create Blacklist / Whitelist restrictions through which end users will only be able to access the privilege which are granted. The policy creation covers Windows/ Linux / Mac OS as part of the scope.
8	The Proposed Solution should be used for the administration of business practices for ensuring strong planning, control, and improvement of an organization's resources and processes.
9	The Proposed Solution should let user can receive these notifications when there is a violation of rules identified by the system. It is based on the user behaviour or if there is a deviation from the normal behavioural characteristics of the user.

10	The Proposed Solution comes with a File Integrity Monitoring which helps administrators monitor or track changes to the most critical or sensitive data. The Proposed Solution should come with a File Integrity Monitoring Tool which helps administrators to monitor or track changes to the most critical or sensitive data.
11	The Proposed Solution should have Data Intellect feature with all the data getting collected from endpoints user of the extensions which is specified in the profiles. After collecting that data, the Data Intellect can classify it into information statistics like exposed data (data has been kept on the shared folder which has not been used for a particular number of days), stale data, etc.
12	The Proposed Solution should be able to Automate profiles which will automates the entire process of applying rules to the users. It should group the users based on their usage history and then assigns the processes that are most frequently used by that group. While Automated Profiling is gathering the data and determining the profiles.
13	The proposed solution should integrate with PAM (Privilege Access Management) in future.
14	The support should be provided for implementation and 5 years post implementation directly from OEM.

General Terms and Conditions	
1	The bidder shall be responsible for providing all materials, equipment's, and services, specified or otherwise, which are required to fulfil the intent of ensuring operability, maintainability, and reliability of the complete equipment covered under this specification within quoted price. This work shall be in compliance with all applicable standards, statutory regulations and safety requirements in force of the date of award of this contract.
2	The bidder shall be responsible for deputing qualified and certified personnel for installation, testing, commissioning, and other services under his scope of work as per this specification. All required tools and tackles for completing the scope of work as per the specification is also the responsibility of the bidder.
3	The bidder shall be responsible for the migration of existing workloads including data to the new solution. Any tools required for the smooth migration shall be used by the successful bidder. Cost for the same shall be borne by the bidder.
4	Product make, model number and part number of each Module/Component to be clearly mentioned in the proposal.
5	Free Updates and Upgrades for Software/Firmware during warranty/contract period.
6	All Components offered in the Bill of Material should be covered under OEM support, enabling program so that to get back-end support / benefits from Principles / OEM in terms of Free Support / Maintenance, if any, Access to 24 x 7 x 365 online support from Technical Assistance Centre of OEM for resolution of problems with the help of their technical team on-site/off-site, advance defective part replacement during warranty period within a period of two working days and OEM Login Access.

Bidders /OEM Eligibility Criteria		
Pre-Qualification/Eligibility Criteria for Bidder		
Sl. No	**Requirement**	**Documents**
1	The bidder should be a company registered under the Companies Act, 1956 or registered firm (Indian/Global) since last 3 years.	Valid documentary proof of Certificate of incorporation, Company registration certificate, Valid GST registration certificate etc to be attached.
2	The bidder must have valid ISO 9001: 2015 and ISO 27001:2013 or higher certifications.	Copy of valid certificates to be attached
3	A copy of at least a single Purchase Order to the value of Rs.100 lakhs or above or Two Purchase Orders each having a value of Rs50 lakhs or Three Purchase Orders each having a value of Rs40 lakhs, during the last three years for any Server/Storage/HCI Solution. Of these at least one project should be for any State/CentralGovernment/Department/Organisation/PSUs/Institutes Government funded.	Valid documentary proof to be provided.
4	A declaration that the bidder has not been debarred/blacklisted by any reputed Government/Semi- Government organization for the quality of services/product and that there is no major complaint against the quality of service/products by any organization.	Self-Certification/ Declaration duly signed by authorized signatory on company letter head.
5	The bidder shall post one Project Manager for management of the project during the execution till acceptance. This person should be qualified and experienced in the installation of the Systems and be authorized to take decisions for smooth and early completion of work.	Self-Certification/ Declaration duly signed by authorized signatory on company letter head.
6	The bidder will be responsible for the Installation, Testing and Commissioning of the solution including migration of Data and VMs from existing infra without any extra cost to NCESS.	Self-Certification/ Declaration duly signed by authorized signatory on company letter head.
7	The bid should preferably be either an Original Equipment Manufacturer (OEM) or should be Authorized System Integrator Partner having Direct Purchase and Support Agreement with the OEM. In case the Bidder is a System Integration Partner of the Principal Manufacturer, a Certificate from the Principal Manufacturer clearly stating the relationship with the Partner and authorization to the Partner to quote for this specific Bid is to be furnished.	Valid documentary proof to be provided.
8	The Bidder should have been actively engaged in the field and shall have a registered office in Kerala for the last three years.	Valid documentary proof to be provided.
9	As per the balance sheets, the bidder must have made profits in the last three financial year's and should be in a sound financial position. Copies of audited balance sheets and IT returns for the last three financial years must be submitted along with the bid. In case, Audited financials are not available for recent financial year, bidder has to upload scanned copy of an undertaking with available financial information. PSUs and Government firms are exempted from compliance to the profit-making clause mentioned above.	Valid documentary proof to be provided.
10	The annual turnover for the last three years of the bidder should be at least Rs.10 Crores.	Valid documentary proof to be provided.
11	The bidder should have a minimum of 2 qualified Engineers in the Server, Storage, Virtualization and Networking domain and should have been in the pay roll of the bidder's firm. Documentary evidence, payroll and CVs of the Engineers must be submitted along with the bid.	Valid documentary proof to be provided.
12	Detailed Bill of Materials (including make, model number of the product and part number of all components) for all the required components should be mentioned else the bidder will be disqualified.	BOM should be Submitted

Pre-Qualification/Eligibility criteria for OEM		
Sl. No	**Requirement**	**Documents**
1	The OEM should have direct presence in India at-least 5 years.	Valid documentary proof to be provided
2	The OEM must have 24 x 7 Technical Assistance centre based in India through a toll-free number.	Valid documentary proof to be provided.
3	The quoted items should be the latest product in the market and launched within three years from the date of publishing this Bid and support for next 7 years should be ensured including hardware and software (Updates and upgrades)	Self-Certification/ Declaration duly signed by authorized signatory on company letter head.

Yours Faithfully,

Sd/-
Deputy Manager (Purchase)