**Turnkey On-premise Cloud Ready Data Centre Unit**

The Indian Statistical Institute (ISI) Kolkata intends to extend its data centre capacity by incorporating a highly available, turnkey data centre unit designed to provide a robust and scalable on-premise cloud infrastructure. The primary goal of this turnkey solution is to establish a private cloud infrastructure that enables efficient management of virtual machines (VMs) and containers, storage, and networking resources in a secure, isolated, and scalable environment.

The system will utilize the widely recognized open-source cloud orchestration platform OpenStack to ensure seamless resource management. This will enable high availability, advanced virtualization capabilities, efficient networking, and resilient storage systems. The architecture will support mission-critical applications that require enhanced data privacy, faster recovery times, and minimized downtime through key features such as live migration and automatic failover.

This scalable solution will be capable of expanding in the future, allowing the easy addition of servers, storage, networking components without affecting overall system performance or uptime. This ensures the continuity of operations and makes the data centre highly resilient to hardware failures, security breaches, or potential disasters.

**Functional Requirements**

| **1** | **Virtualization**  **Management**: | The system will manage multiple virtual machines and containers, ensuring optimal performance and resource allocation.  Supports load balancing and minimizes downtime through built-in virtualization failure protection. |
| --- | --- | --- |
| **2** | **High Availability**: | The architecture will ensure seamless failover between nodes in case of hardware or software failure, guaranteeing the availability of the cloud environment with minimal downtime.  Redundant components (servers, networking) will prevent single points of failure. |
| **3** | **Live Migration**: | Enables live migration of workloads between servers without service interruptions, ensuring smooth transitions during maintenance or hardware failures.  Enhances the system's resilience to disruptions by allowing ongoing operations during server migrations. |
| **4** | **Resilient Storage**: | Seamlessly integrates both local and enterprise-level storage solutions, including block, object, and file storage systems.  Ensures data redundancy and fault tolerance through data replication across multiple nodes, enhancing overall storage reliability. |
| **5** | **Advanced Networking**: | Supports software-defined networking (SDN) for flexible, dynamic network configurations, allowing network segmentation, policy management, and bandwidth optimization.  Provides enhanced security features such as virtual private clouds (VPCs) and network isolation. |

| **6** | **Disaster Recovery**: | Automated backup and recovery systems are integrated to ensure rapid restoration in the event of major failures or data loss incidents.  Protects against data corruption or loss by regularly creating snapshots of the system. |
| --- | --- | --- |
| **7** | **Scalability**: | Easily scalable infrastructure that allows the addition of more servers, storage, and networking components as needed without service disruptions.  Future-proof design to accommodate growth, ensuring long term sustainability and adaptability for increasing workloads. |

**Hardware Requirements:**

To implement the proposed turnkey data centre unit, the following hardware components may be installed to provide a robust and reliable foundation for the proposed private cloud infrastructure, ensuring high performance, easy scalability, and secure connectivity for the ISI-Kolkata data centre expansion.

| 1 | **Servers (4 Units)**: | High-performance servers equipped with multi-core processors, ample RAM, and sufficient storage to support virtualization and containerized workloads. Each server should have redundant power supplies and hot-swappable components for added resilience and ease of maintenance. For detailed specification see Annex II & III |
| --- | --- | --- |
|  | **NetworkSwitches(2 Units)**: | Two high-end, rack-mounted switches with multiple gigabit and 10G Ethernet ports to provide high-speed, redundant network connectivity between servers, storage, and other data centre components. These switches should support advanced features like VLAN segmentation, link aggregation, and software-defined networking (SDN) integration. For detailed specification see Annex IV |
|  | **Firewall (1 Unit)**: | A small, rack-mounted firewall capable of providing essential security features such as network segmentation, intrusion prevention, and stateful packet inspection to protect the cloud infrastructure. The firewall should have high throughput to handle traffic between the internal and external network, with support for VPN connectivity if required. For detailed specification see Annex I |
|  | **KVM Switches**: | Rack-mounted keyboard, video, and mouse (KVM) switches to enable easy management and direct control of multiple servers from a single console, reducing space and cabling complexity within the rack. |
|  | **Rack Enclosure**: | A standard 42U rack to securely house the servers, switches, firewall, and other data center components. The rack should be equipped with sufficient ventilation, cooling, and cable management options. |
|  | **Peripheral Connectors and Cables** | All necessary peripheral connectors, including power cords, rackmount kits, and power distribution units (PDUs) to ensure safe and organized power delivery to all devices. |
|  | **Networking Cables**: | A sufficient number of CAT6 or higher-grade Ethernet cables, along with SFP+ or fibre optics cables for high-speed interconnections between switches and servers. All cables should be neatly organized with cable ties or trays for easy maintenance and airflow management. |

**Scope of Work:**

1. **Supply, Installation, Configuration, and Integration**: The bidder shall supply the required hardware as specified in the hardware requirements section, which includes 4 nos servers, 2 nos high-end switches, 1 no firewall and 1 no KVM switches. The bidder will also be responsible for installing and configuring OpenStack and its components to achieve the functional requirements outlined in the proposal. The system must support private cloud functionality using OpenStack, ensuring scalability, virtualization, networking, and storage capabilities. The solution will be installed at CSSC, 4th Floor, SN Bose Bhavan, ISI Kolkata - 700108.

2. **Commissioning and Support**: The turnkey solution must be fully commissioned, with the bidder providing 3 years of comprehensive support post-installation, including enterprise-level 24x7 support for hardware and software components. Proof of warranty and OEM-backed support must be submitted, ensuring no limitations on enterprise support agreements.

3. **Integration with Existing Infrastructure**: The solution should be integrated seamlessly with ISI Kolkata's current data center and network infrastructure, including existing security appliances, ensuring compatibility and enhancing system performance.

4. **OEM Engagement**: The bidder must ensure active engagement of the OEM during implementation and throughout the support period, with direct warranty agreements and enterprise support executed in the name of ISI Kolkata for the project.

5. **Quality Assurance and User Acceptance Testing (UAT)**: The bidder must conduct Quality Assurance testing of the entire system and assist ISI Kolkata in performing User Acceptance Testing (UAT) to validate the solution’s performance and reliability.

6. **Training and Documentation**: The bidder shall provide comprehensive post implementation training to ISI Kolkata personnel on managing, operating, and maintaining the system. The bidder will deliver all relevant project documentation, including standard operating procedures (SOPs), system designs, and manuals. All documents must be vetted by the respective OEMs before final acceptance.

7. **Post-Implementation Support**: Post-implementation support must be provided by trained engineers for ongoing system management, issue resolution, and troubleshooting. Onsite support should be available as needed, with priority response for critical issues.

8. **Software Licensing and Handover**: The bidder is responsible for providing all necessary software licenses for the cloud orchestration platform and associated tools. The solution must be fully implemented, tested, and handed over to ISI Kolkata officers, with ongoing support provided for updates, upgrades, configuration changes, and troubleshooting.

9. **Enterprise Warranty**: All supplied systems, including servers and switches, must be covered under an enterprise-level, comprehensive onsite warranty for 5 years, ensuring hardware and software issues are resolved without delay.

10. **Scalability and License Extension**: ISI Kolkata reserves the right to extend the quantity of user licenses and resources for the proposed solution at the same rate

during the contract period. The system should be scalable to accommodate future growth without impacting performance.

11. **Conflict Resolution**: In case of any conflict between the terms mentioned in the GeM Catalogue Specification and those specified in the ATC (Additional Terms & Conditions), the details in the ATC will take precedence. The technical evaluation will be conducted based on the ATC conditions.

By adhering to this Scope of Work, the selected bidder will deliver a fully integrated, highly available, and scalable turnkey data center unit, ensuring ISI Kolkata’s cloud infrastructure meets both current and future demands.

**Annexure I**

| **Firewall** | |
| --- | --- |
| **Quantity: 01** | |
| Make/Model | Industry leading OEMs |
| Firewall Throughput | 500Mbps |
| UTM Throughput | 300Mbps |
| DPI-SSL Throughput | 150 Mbps |
| New connections/second | 5000 |
| Concurrent connections (SPI) | 75,000 |
| Concurrent connections (DPI) | 50,000 |
| Port Configuration | 8 x 1 GbE, Configurable |
| 1 x Console Port |
| VPN | Site-to-Site |
| SSL |
| Management/Monitoring | CLI, SSH, Web UI |
| Certifications | RoHS |
| Warranty | 5 years on-site |

**Annexure II**

| **Type - 1 Server** | |
| --- | --- |
| **Quantity: 02** | |
| Make/Model | Reputed OEM |
| Processor | 1x Intel Xeon 65XX series or AMD EPYC 9xx4 series 32 core processor, and L3 cache at least 60MB, and Base frequency at least 2.2 GHz having SPECrate2017\_int\_base score at least 310 and SPECrate2017\_fp\_base score at least 400 |
| Chipset | Should support 02 no of above specified processor , Should have 32 DIMMM slots, should support 8TB RAM, should support 120 CPU cores, Should have 8 PCIe slots |
| RAM | 128 GB DDR5 5600 MHz ECC |
| Storage | SSD 6 TB (2 x 1 TB + 2 x 2 TB) |
| SAS/SATA 12TB (4 x 3 TB/6 x 2 TB) |
| Should be equipped with a 12Gbps RAID controller (from same OEM) with 8GB nonvolatile cache capable of building RAID using mixed type drives (HDD and SSD) simultaneously and supporting different RAID types simultaneously |
| Power Supply | 80Plus Platinum rated 2200 W, Hot plug, Fully Redundant Power Supply |
| Fan | Fully redundant hot swappable Fan systems |
| Network  Interface | 2 x 10 G SFP+, 2 x 1/10 G Base-T with additional 1G base T dedicated management port |
| Form Factor | 1U Rack mountable |
| Security | 1. Silicon-based Hardware Root of Trust.  2. Automatic BIOS recovery.  3. Firmware drift detection & alerting.  4. Cryptographically signed firmware updates.  5. Cryptographically verified trusted booting standards meeting NIST SP 800- 147B, protection standards meeting NIST SP 800-193 standards & secure media sanitization standards meeting NIST SP 800-88.  6. System lockdown support to lock down configuration and firmware, protecting the server from inadvertent or malicious changes.  7. Secure default passwords during transit. Persistent event logging including user activity.  8. Drive security, including secure system erase for HDD, SSD & NVMe. 9. Protection against compromised firmware execution.  10. UEFI secure boot with custom certificates.  11. Intrusion alert in case chassis being opened. |
| OS  Compatibility | RHEL, Ubuntu, Windows Server, KVM, and VMware |
| Management | 1. The system should provide comprehensive monitoring of critical components, including the fan, power supply, memory, CPU, RAID, and NIC, with proactive reporting for impending failures.  2. All updates must be carried out using the OEM's access controller and management software to ensure security.  3. The system management software should support at least (but not limited to) virtual media, virtual folders, remote file sharing, and virtual consoles. 4. The integrated remote access controller must enable advanced agent-free local and remote server administration, offering capabilities such as configuration management, firmware updates, OS deployment, health monitoring, diagnostics, and the automation of routine management tasks, all backed by a perpetual license.  5. The system management software should provide a RESTful interface for the management of appliances through implementing Redfish standards. |
| Certifications | ISO/IEC 27001, UL, RoHS |
| Warranty | 5 years on-site |

Higher values in context of all kinds of performance and capacity metrics will also be

Note:

accepted.

**Annexure III**

| **Type - 2 Server** | |
| --- | --- |
| **Quantity: 02** | |
| Make/Model | Reputed OEM |
| Processor | 2x Intel Xeon 65XX series or AMD EPYC 9xx4 series 32 core processor, and L3 cache at least 60MB, and Base frequency at least 2.2 GHz having SPECrate2017\_int\_base score at least 310 and SPECrate2017\_fp\_base score at least 400 |
| Chipset | Should support 02 no of above specified processor , Should have 32 DIMMM slots, should support 8TB RAM, should support 120 CPU cores, Should have 8 PCIe slots |
| RAM | 128 GB DDR5 5600 MHz ECC |
| Storage | SSD 6 TB (2 x 1 TB + 2 x 2 TB) |
| SAS/SATA 12TB (4 x 3 TB/6 x 2 TB) |
| Should be equipped with a 12Gbps RAID controller (from same OEM) with 8GB nonvolatile cache capable of building RAID using mixed type drives (HDD and SSD) simultaneously and supporting different RAID types simultaneously |
| Power Supply | 80Plus Platinum rated 2200 W, Hot plug, Fully Redundant Power Supply |
| Fan | Fully redundant hot swappable Fan systems |
| Network  Interface | 2 x 10 G SFP+, 2 x 1/10 G Base-T with additional 1G base T dedicated management port |
| Form Factor | 1U Rack mountable |
| Security | 1. Silicon-based Hardware Root of Trust.  2. Automatic BIOS recovery.  3. Firmware drift detection & alerting.  4. Cryptographically signed firmware updates.  5. Cryptographically verified trusted booting standards meeting NIST SP 800- 147B, protection standards meeting NIST SP 800-193 standards & secure media sanitization standards meeting NIST SP 800-88.  6. System lockdown support to lock down configuration and firmware, protecting the server from inadvertent or malicious changes.  7. Secure default passwords during transit. Persistent event logging including user activity.  8. Drive security, including secure system erase for HDD, SSD & NVMe. 9. Protection against compromised firmware execution.  10. UEFI secure boot with custom certificates.  11. Intrusion alert in case chassis being opened. |
| OS  Compatibility | RHEL, Ubuntu, Windows Server, KVM, and VMware |
| Management | 1. The system should provide comprehensive monitoring of critical components, including the fan, power supply, memory, CPU, RAID, and NIC, with proactive reporting for impending failures.  2. All updates must be carried out using the OEM's access controller and management software to ensure security.  3. The system management software should support at least (but not limited to) virtual media, virtual folders, remote file sharing, and virtual consoles. 4. The integrated remote access controller must enable advanced agent-free local and remote server administration, offering capabilities such as configuration management, firmware updates, OS deployment, health monitoring, diagnostics, and the automation of routine management tasks, all backed by a perpetual license.  5. The system management software should provide a RESTful interface for the management of appliances through implementing Redfish standards. |
| Certifications | ISO/IEC 27001, UL, RoHS |
| Warranty | 5 years on-site |

Higher values in context of all kinds of performance and capacity metrics will also be

Note:

accepted.

**Annexure IV**

| **Technical Specification of Layer-3 Switch** |
| --- |
| **Quantity: 01** |
| **Physical Requirements** |
| 1. The switch should be 1/2U 19" Rack Mountable. |
| 2. The switch should have dual, redundant, field-replaceable, hot-swappable power supplies and fans with front-to-back airflow. Should have at-least 4 Fan modules and 2 power supplies installed from day 1. |
| 3. The switch should have 48 ports of 10GbE/25GbE (SFP+/SFP28). The switch should be populated with atleast 6 Single Mode and 24 Multi Mode enterprise grade transceivers from same OEM from day 1. |
| 4. The switch should have minimum 4 ports of 40GbE/100GbE (QSFP+/QSFP28). |
| 5. The switch should have RJ-45 serial and USB console port. Separate RJ-45 Ethernet Management port should be present for out-of-band management. |

| **High Availability** |
| --- |
| The switch should be configured with standby systems (Active-Active) in order to achieve high availability. |
|  |
| **Performance Requirements** |
| 1. The switch should have minimum of 4 cores (64bit), 1.8 GHz processing unit. |
| 2. The proposed switch should have minimum 16GB RAM, 16GB Flash Memory. |
| 3. Should support unified packet buffer size of atleast 32MB. |
| 4. Switch should have minimum 3.2 Tbps switching capacity. |
| 5. Switch architecture should be able to achieve 1 Bpps forwarding rate. |
| 6. The switch ports should support Jumbo Frames of size upto 9K bytes. |
| 7. The switch should have minimum 50K MAC Address Table size. |
| 8. The switch should support minimum 120K IPv4 routes, 80K IPv6 Routes and 4K IPv4/IPv6 Multicast Routes. |
| 9. The switch should support minimum 25K IPv4 ACLs and 12K IPv6 ACLs. |

| **Functional Requirements** |
| --- |
| 1. The switch should support Spanning Tree Protocol (STP/RSTP/MSTP) with Root Guard. |
| 2. The switch should support Ethernet Ring Protection Switching (ERPS) and Unidirectional Link Detection (UDLD) |
| 3. The switch should support eight egress queues per port for different types of traffic |
| 4. The switch should support switch virtualization feature that allows links, physically connected to two different switches, to appear as a single port channel |
| 5. The switch should support layer 2 QoS mechanism like 802.1p or equivalent |
| 6. The switch should support Link Aggregation Control Protocol (LACP). |
| 7. The switch should support Precision Time Protocol or equivalent to synchronize clocks with sub-microsecond accuracy across devices in a network. |
| 8. The switch should support atleast 4000 IEEE 802.1Q VLANs. |
| 9. The switch should support Private VLAN for traffic isolation within a particular VLAN. |
| 10. The switch should provide storm protection to limit unknown broadcast, multicast, or unicast storms with user-defined thresholds. |

11. The switch should support Strict Priority (SP) queuing, explicit congestion avoidance features and Access Control Lists (ACLs) for both IPv4 and IPv6 traffic.

| 12. The switch should support Internet Group Management Protocol (IGMPv1, v2, and v3) and Multicast Listener Discovery (MLDv1 and v2). |
| --- |
| 13. Should support hardware accelerated MACSEC-256 encryption algorithm with static key provisioning enabling secure communication. |
| 14. The switch should support static VXLAN as well dynamic VXLAN with BGP EVPN(Should also support multicasting) |
| 15. The switch should support IPv4 and IPv6 Static Routing. |
| 16. The switch should support Open shortest path first (OSPF) for IPv4 and IPv6. |
| 17. It should support VRRP or equivalent , enabling switches to work together for dynamic backup and ensuring a highly available routing environment. |
| 18. Should support Virtual routing and forwarding (VRF) to allow multiple instances of a routing table to co-exist within the same router |
| 19. The switch should support Border Gateway Protocol 4 (BGP) for IPv4 and IPv6. |
| 20. The switch should support Policy Based Routing (PBR). |
| 21. The switch should support Multicast Routing using PIM-SM/SSM |
| 22. The switch should support DHCP Server providing DHCP services (for IPv4 and IPv6). |
| 23. The switch should support Equal-Cost Multipath (ECMP). |
| 24. Switch should support secure boot feature e.g. during system boots, the system’s software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic. |
|  |
| **Switch Management Requirements** |
| 1. The switch should support SSH, SNMP and Remote monitoring (RMON). |
| 2. The switch should support sFlow or equivalent for traffic analysis. In general switch should have in built features for monitoring, as well as troubleshooting network issues and related metrics |
| 3. The switch should support RADIUS and TACACS+ for securing administrative access. |
| 4. The switch should have Command Line Interface (CLI) with a hierarchical structure. |
| 5. The switch should be programmable via declarative style scripting or model centric programmability |
| 6. The switch should be manageable from third-party On-premises NMS solution. |
| **Compliance Requirements** |
| 1. The switch should have RoHS compliance |
| 2. The device should be IPv6 ready certified from day one. |
| **Support and Warranty Requirements** |
| 1. The switch shall be offered with minimum five (05) years comprehensive warranty with 24x7 Technical support from OEM directly. Warranty must include Same-day Rapid Dispatch of Parts and advanced RMA. |
| 2. All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1. |

**Annexure V**

| **KVM Switch** | |
| --- | --- |
| **Quantity: 01** | |
| Make/Model | Industry leading OEMs |
| Form Factor | Rackmount LCD Console with Keyboard and TouchPad, |
| Display | 17’’ 1280 x 1024 @ 75 Hz |
| Number of host | 8 |
| USB support | Yes |
| Access control | Password and optional fingerprint |
| Auto scan mode | Hot pluggable - add or remove computers without having to power down the switch |
| Daisy Chain | Yes, up to 16 additional units, supporting at least 128 hosts |
| Supported OS Platforms | Windows, Linux |
| Support for external mouse | Yes |
| Warranty | 5 years on-site |

**Annexure VI**

| **Server Rack** | |
| --- | --- |
| **Quantity: 01** | |
| Make/Model | Industry leading OEMs |
| Mount Type | Floor Mount Server Rack with lockable castor wheels |
| Size | 19”, 42U, other dimensions should be suitable to install the quoted servers, switch and KVM switch |
| Material | Powdered coated steel body, toughened glass doors |
| Door type | Swivel type, minimum 180-degree, front and rear glass doors |
| Side panels | Removable, steel side panels |
| Lock type | Combination lock, single key for front and rear door locks |
| Ventilation | 4 nos of installed fans on top panel |
| Accessories | 1. Should have at least one power strip with 8 sockets, compatible with 16A, India, power cords  2. Should have vertical cable manager |
| Warranty | 5 years on-site |