



काठमाण्डौ उपत्यका खानेपानी लिमिटेड

मुख्य कार्यालय

सूचना प्रविधि शाखा



मिति: २०८३-०६-२७

ने.स. ११४६ कौलाथ्व तृतिया, मंगलबार

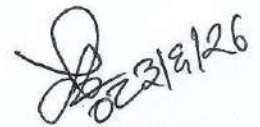
विषय: लागत अनुमान तयारीको लागि दररेट उपलब्ध गराईदिने बारे

उपरोक्त सम्बन्धमा यस कम्पनीका लागि यसै साथ संलग्न स्पेसिफिकेसन बमोजिमको Procurement of Private Cloud Services including Network, Security, and Maintenance Services खरिद गर्नुपर्ने भएकोले सोको लागत अनुमान तयारीको लागि यस कम्पनीको मौजुदा सूचिमा सूचिकृत सूचना प्रविधि सम्बन्धि (डाटा सेन्टर / क्लाउड सेवा) कार्य गर्ने सेवा प्रदायकहरूले के कति दर रेटमा सेवा उपलब्ध गराउने हो ? सो सेवाको दररेट यो सूचना प्रकाशित भएको मितिले ३ दिनमा (मिति २०८३-०६-२९ सम्म) कार्यालय समय भित्र संलग्न ढाँचामा उपलब्ध गराईदिनुहुन यो सूचना कम्पनीको वेबसाईटमा प्रकाशित गरिएको छ।

तपसील:

SN	Particulars	Unit	Quantity	Rate without VAT(NRs.)
1	Procurement of Private Cloud Services including Network, Security, and Maintenance Services	Month	1	

दर रेट पेश गर्नुपर्ने स्थान: सूचना प्रविधि शाखा



ई. पुर्ण बहादुर कुवर

प्रमुख

सूचना प्रविधि शाखा

Technical Specifications for the Procurement of Private Cloud Services including Network, Security, and Maintenance Services		
SN	Particulars	Requirement
1	Private Cloud's Environment	The private cloud service provider should provide a minimum of 168 Physical core Platinum Processors.
		The private cloud service provider should provide a minimum of 768GB RAM.
		The private cloud service provider should provide minimum of 15 TB of NVMe Solid State Drive (SSD) for Primary storage of the Private Cloud Solution offered.
		The system should be able to support Windows or Ubuntu Operating System.
		The private cloud service provider should provide high performing enterprise level hardware resources to increase the performance of KUKL applications.
		The private cloud service provider must ensure that the hosting environment has redundant Internet and Intranet Connections.
		The private cloud service provider must propose an environment which ensures the architecture in which Application Server, Database Server, Development, UAT, Production Server and test environment are logically separated. KUKL must approve this architecture before implementation.
		The private cloud service provider must provide backup and replication service as mentioned in Data Backup and Retention section.
		The private cloud infrastructure should have physical security, rodent protection, redundant internet and intranet connectivity, video surveillance and power supply.
		The private cloud solution must have dedicated bare metal servers.
		The virtualized environment in the cloud solution must be in High Availability (HA) mode. The private cloud service provider must ensure host level failovers, with minimum 3 physical nodes with redundant equivalent dedicated for KUKL private cloud.
		The virtualization solution should be active licensed enterprise level and should not be open source. Licence should be valid throughout the contract period.
		The private cloud service provider must have their own Datacenter and managed services solutions.
		The data center (DC) where the cloud service is hosted should be operating within Nepal. DC should be inside Kathmandu valley and Disaster Recovery (DR) should be outside Kathmandu valley in different seismic zone.
		The subscribed backup space should be accessible from both private cloud DC and private cloud DR.
		The private cloud should be accessible/integration with existing KUKL Network/Hardware infrastructure.
		The private cloud service provider should integrate KUKL's procured internet and intranet connectivity and establish L2 connectivity among the offices/locations of KUKL. So that the offices/locations of KUKL can connect to the private cloud using L2 connectivity and procured internet also should be distributed to the offices/locations of KUKL using L2 connectivity.
		The private cloud service provider should provide at least 1G connectivity from private cloud to KUKL instructed locations.
		The Bidder should provide datasheet of the proposed bare metal server and Virtualization solution.
2	Private Cloud's Security	The private cloud service provider should provide dedicated Next Generation Firewall (NGFW) services to KUKL private cloud. The appliance should be Hardware. The NGFW should be on HA mode.
		The proposed firewall should be listed as a Leaders in Gartner's Magic Quadrant for Network Firewall.
		The Minimum bandwidth requirement for the dedicated firewall should not be less than 1.5 Gbps of NGFW traffic throughput.
		The proposed security service should be robust and scalable with sufficient performance that can sufficiently handle Branch Offices/locations through VPN connection.
		The proposed service should support routing protocols such as: static Routes, OSPF, BGP.
		The proposed Firewall system should support a minimum of 100,000 concurrent sessions.
		The proposed service should have botnet protection and should prevent clients from contacting Command and Control (C&C)Server.
		The private cloud service provider should also provide security for web applications hosted in the private cloud solution.
		The private cloud solution must have a firewall as a service.
		The private cloud solution must have an Intrusion Detection System (IDS) / Intrusion Prevention System (IPS).
		IDS/IPS should monitor network traffic in real time and detect potential security threats, signature based/anomaly-based detection for known/unknown attacks.
		IDS/IPS should be scalable to handle large network environments.
		The propose solution should have alert generation, automatic blocking of malicious traffic, Stateful inspection of incoming and outgoing network traffic and Rule based filtering to control access to network resources as per request made by KUKL.
		The private cloud service provider should update the rules of Firewall/IDS as instructed by KUKL.
		The private cloud service provider must provide firewall configuration for KUKL in KUKL's desired format as per KUKL's request.
		NGFW license must be valid throughout the contract period
		The Bidder should provide datasheet of the proposed NGFW solution.
3	Disaster Recovery(DR)	The private cloud service provider should also provide managed DR site for the proposed Private Cloud solution.

	Service	The Virtual Machine (VM) in DC should be replicated to DR site using private cloud service provider 's replication technology.
		The Replication duration of virtual machine should not be more than 30 Minutes.
		The DR Service should be able to run the mentioned application when Private Cloud's main DC is unavailable. KUKL should be able to use the application from DR Service in case of unavailability of Private Cloud's main DC.
		SSL VPN should be configured so that the offices/locations of the KUKL can access the application running on the DR Service.
		At least quartly DR drill should be done by privite cloud service provider to ensure the availability of service from DR.
		The Bidder should provide datasheet of the equipment proposed in DR solution.
4	Data Backup and Retention	The private cloud solution must have a robust backup and recovery plan for at least 25 Virtual Machines.
		Daily incremental backup or daily differential backup, once a day
		Weekly full backup, once a week and store in subscribed backup storage in the private cloud.
		Monthly full backup of earlier months and store in subscribed backup storage in the private cloud.
		At total should provide 12 monthly backups, 4 weekly backups of current month and 7 incremental backup images for the current week. These backups should be accessible to KUKL IT section for restoration and data integrity checks.
		The private cloud service provider should take data backup, maintain and delete as per KUKL instructions.
		The private cloud solution should have 1 hour of RTO (Recovery Time Objective) and 30 minutes of RPO (Recovery Point Objective).
		KUKL may instruct from time to time for addition of backup location. The private cloud service provider must comply with the request and send one copy of the backup to the instructed location.
		The private cloud infrastructure should have backup systems in place to backup data, installed Virtual Machine and other items as instructed by KUKL. The system should be able to restore the VM and data in case of failures.
		The private cloud service provider should create data backup from the private cloud system to subscribed backup system present in the private cloud and to the location instructed by KUKL.
		Backup of the cloud solution includes but not limited to virtual machine, application, databases. KUKL may instruct from time to time for the addition of the number of items to be backed up.
		One copy of the backup should be sent to the location provide by KUKL. KUKL should be able to open the backup copy and restore without any assistance from the private cloud service provider .
		Private cloud service provider must provide a copy of daily,weekly,monthly backup for 1 year to the separate dedicated storage device apart from the allocated 15TB for KUKL in Datacenter (DC).
		Privite cloud service provider must provide one copy of daily, weekly, monthly for one year backup to the separate dedicated storage device in the another Near Datacenter(NDC) which must be in different district/25km far from the main DC within Kathmandu valley.
5	Web Application Security(WAF) as a Service	The Bidder should provide datasheet of the proposed data backup solution.
		The Bidder should provide datasheet of the proposed deligated storage device apart from the allocated 15TB for KUKL DC and NDC.
		Comprehensive protection against OWASP (Open Web Application Security Project) top 10 vulnerabilities and zero-day exploits.
		API security with auto-discovery, schema enforcement, and rate-limiting capabilities.
		Advanced bot mitigation with the ability to distinguish between legitimate and malicious bots.
		Layer 7 DDoS mitigation to safeguard against volumetric floods and slow-rate attacks.
		TLS/SSL termination with support for TLS 1.3.
		Virtual patching capability for rapid protection against new threats.
		Geo-blocking and IP reputation-based filtering.
		System shall support a minimum sustained throughput of 200 Mbps after HTTPS Layer-7 SSL/TLS offloading and scalability up to 1 Gbps
		Support for at least 100,000 requests per second (RPS).
		Additional latency of less than 50 milliseconds globally.
		The provider must have an operational presence in Nepal.
		Service must meet an availability commitment backed by SLA of at least 99.96%.
		Enterprise-Grade Licensed WAFs (Non–Open Source)
		Continuous 24x7x365 monitoring and real-time threat mitigation.
		Creation, tuning, and regular updating of rule sets.
		Distributed Denial-of-Service (DDoS) protection application layer (Layer 7).
		Periodic reviews of the security posture and provision of detailed reports.

		Private Cloud Service Provider should provide dedicated dashboard for KUKL The proposed WAF solution shall be a genuine, fully licensed product, with all required licenses, security subscriptions, updates, and technical support valid and continuously maintained throughout the entire contract tenure. The proposed WAF solution can be physical or virtual appliance. The Bidder should provide datasheet of the proposed WAF service. Logging and Reporting - Real-time traffic visibility detailing attack types, sources, and mitigation actions taken. - Retention of a minimum of 90 days of online logs with archival storage for at least one year. - Export of reports in standard formats such as CSV, JSON, and PDF.
6	SIEM (Security Information and Event Management) as a Service	Scope of Work - Collect, normalize, and analyze security logs from all assets (minimum 25 VMs). - Correlate events across multiple sources to detect threats in real time. - Provide dashboards, alerts, and compliance-oriented reporting. - Support integration with existing private cloud infrastructure, security tools, and applications. - Be scalable to support future asset growth. - Dedicated dashboard should be provided. - The proposed SIEM solution shall be a genuine, fully licensed product, with all required licenses, security subscriptions, updates, and technical support valid and continuously maintained throughout the entire contract tenure. - The private cloud service provider must have their own SOC (Security Operation Center) team with qualified professional's for monitoring and incident reporting. - The proposed solution can be physical or virtual appliance. - The Bidder should provide datasheet of the SIEM service. Functional Requirements Log Management - Centralized log collection from servers, applications, network devices, firewalls, IDS/IPS, and endpoints. - Secure log storage with tamper-proof mechanisms. - Log retention configurable per compliance needs (minimum 3 months). Event Correlation & Analysis - Real-time correlation of events across at least 25 VMs. - Automated threat detection (malware, brute force, insider threats, privilege escalation). - Predefined correlation rules with flexibility to add custom rules. Alerting & Monitoring - Real-time alerting with configurable severity levels. 24/7 monitoring dashboard with drill-down capabilities. - Integration with email, SMS, or ticketing systems for incident alerts. Reporting & Compliance - Pre-built compliance reports to support security monitoring, audit and compliance requirements in accordance with applicable standards and regulatory frameworks. - Customizable reporting with scheduling options. - Audit-ready event tracking. Integration & APIs - API support for integration with third-party tools (ticketing, vulnerability scanners, SOAR). - Compatibility with hypervisors, private cloud orchestration tools, and security appliances. - SIEM integration with multiple SIEM solutions. Security Operations Support - Threat intelligence feed integration (global and local indicators of compromise). - Forensic analysis tools. - User and Entity Behavior Analytics (UEBA) as an add-on option.
7	Support and Quality of Service (QoS)	The private cloud service provider should provide support Help desk service to deal with issues related to the private cloud infrastructure and connectivity. The private cloud service provider should provide the services and support 24 x 7 x 365 days.

		The private cloud service provider should provide Dashboard for Resources Utilization monitoring of Services of private cloud.
		The private cloud service provider should be responsible for coordinating with designated person/department/division/branch/section of KUKL to solve connections problems at Head Office and branches/locations arising from time to time.
		The private cloud service provider should be responsible for serving clients with configuration of VPN Connection between hosting environment and client Head Office and its branch offices.
		The private cloud service provider should provide 5 minutes response time and call escalation matrix for business criticality.
		The private cloud service provider should create virtual machines, install operating systems, migrate the current applications of the KUKL including the databases to the private cloud and as instructed by KUKL (without any extra cost) from time to time.
		The private cloud service provider should maintain the connectivity between physical infrastructure present in the KUKL and private cloud infrastructure using VPN or any other method (without extra cost).
		The private cloud service provider should set up/configure the system/environment such that KUKL should be able to run the entire system (Billing, New Connection, HR, Account, Inventory & Asset, Grievance, Portal, Mobile APP, Email, Website, etc.) from the KUKL offices or configure as per KUKL instruction.
		The private cloud service provider should also configure remote access VPN for accessing the hosted software and server from a remote location.
		The private cloud service provider must have a minimum of 99.9% uptime.
		The private cloud service provider should provide Access Log/Error Log of the private cloud infrastructure as per the client's need.
		The private cloud service provider should provide a security incident report that occurred inside the private cloud infrastructure procured by KUKL.
		The private cloud service provider should provide and manage all VPS services (like DNS, software, email, etc.).
		The private cloud service provider should be responsible for management, monitoring, maintenance, troubleshooting of DNS and email server hosted in cloud VM. The private cloud service provider should ensure the continuous availability and proper functioning of these and provide technical support as required.
		The private cloud service provider should provide KUKL access for PAM (Privilege Access Management) integration in the private cloud service if needed.
		The private cloud service provider should all to conduct Vulnerability Assessment and Penetration Testing (VAPT)/ Information Security/System Audit and improve the private cloud service as recommended.
		The private cloud service providers should have service downtime notification and escalation options.
8 Documents Required		The bidder should submit document regarding their own company operating a Datacenter.
		The bidder should submit the datacenter and cloud center registration document provided by the Department of Information Technology (Recently named as Information Technology and Digital Governance Office) under the "Data Center and Cloud Services (Operation and Management) Directive, 2081".
		The bidder should submit the ISO/IEC 27001 certification document of the proposed datacenter.
		The bidder should submit technical datasheet as per specification.
9 Network Management Service		The service provider should managing and maintaining the whole KUKL infrastructure from the data center (private cloud) to the firewall of the branches/offices/locations of KUKL.
		All Configuration done on the firewall and networking device should be provide to the KUKL in the form of digital copy or as demanded by the client.
		The service provider should manage the networking devices located in the private cloud.
		The service provider should also manage the network connectivity (L2 and L3) from the datacenter to the offices/branches/locations of KUKL or as mentioned by KUKL
		The service provider should provide the network support services for 24 x 7 x 365 days.
		The service provider should manage and provide network support to the current operating and future increased sites/location of KUKL. Current operating sites/locations are 30 and may increase up to 60.
10 System/Server Management		The service provider should manage and maintain KUKL Systems/Software and server located in the private cloud.
		The private private cloud service provider should provide the system/server support services for 24 x 7 x 365 basis.
11 Cloud Migration		The service provider should perform migration of all KUKL VM, applications, databases, data and related services from the existing private cloud environment with less than 30 minute downtime. Migration task should be done offhour.
		The service provider should migrate all the existing production, brackup and DR data which may increase the current data size. The current data size is 9 TB in production, 12 TB in backup in DC having 12 VMs and 9 TB in DR site. The Bidder/service provider should migrate these all data from existing environment to new private cloud environment.
		The private service provider should submit a detailed migration plan covering migration methodology, connectivity, establishing secure network, Data integrity testing, validation, and rollback procedures, including dedicated high-throughput connectivity of minimum 10 Gbps between the existing and proposed private cloud environments for migration.
		All necessary network and security infrastructure, including switches, firewalls and related equipment, required for migration shall be provided by the successful bidder, and all data transferred during migration shall be protected using secure communication protocols and encryption in transit.

		The migration should be complete within 30 days of the contract date.
12	End Point Security	The private cloud service provider must provide active license endpoint security with Data Loss Prevention(DLP) for each VM.
13	Window server	The private cloud service provider must provide at least 40 core of windows server standard licenses. The windows server version should not be in the end of support.
14	Public IP	The private cloud service provider should provide and manage at least 10 dedicated public IPs.
15	Domain Management Service	The private cloud service provider should manage and provide the domain kathmanduwater.com with SSL certificate. The domain should be register/modify under it@kukl.org.np email.
16	Ticketing System	The private cloud service provider should provide and maintain a dedicated ticketing and support management system for recording, monitoring, tracking, and resolving service requests, incidents, complaints, and technical support issues throughout the contract period.
17	Training to KUKL IT Employee	The private cloud service provider should provide 10 working days of training for Kathmandu Upatyaka Khanepani Limited's IT section staff regarding the operation of cloud services, security and network connectivity.
		The training should provide withing 3 month from the service start date.