सत्यमेव जयते

EMBASSY OF INDIA
545-547, Merchant Street
Post Box No. 751
Yangon, Myanmar
Tel: (951) 391219, 243972, 388412
Fax: (951)254086, 250164, 388414
Email: hoc.yangon@mea.gov.in

No. YAN/ISI/305/02/2004-II

22.05.2017

Subject: Proposal for Redevelopment, Upgradation and VPC web hosting of the website of the Embassy of India, Yangon

The website of the Embassy of India, Yangon intends to redesign, upgrade its multilingual website, change the domain name of present website www.indiaembassyyangon.net and migrate to a Virtual Private Cloud (VPC) with data centre in India as per MEA guidelines. The website should be redesigned and developed as per SQT Certification and MEA design. The preferred domain name for new website is: www.indianembassyyangon.in

Reputed firms having experience in developing website of Indian Embassy/Consulate abroad may send their proposal along with supporting documents to Head of Chancery, Embassy of India, 545-547 Merchant Street, Yangon, Myanmar (hoc.yangon@mea.gov.in) by 5 p.m. on 31st May 2017.

The Embassy reserves the right to accept or reject any proposal.

(Shweta Singh)
First Secretary & Head of Chancery

No. YAN/ISI/305/02/2004-II 22.05.2017

EMBASSY OF INDIA
YANGON

Subject: Proposal for Redevelopment, Upgradation and VPC web hosting of the website of the Embassy of India, Yangon

1.0 OBJECTIVE

1.1 To redesign, develop as per SQT Certification and MEA design, maintain and migrate Mission's multilingual portal www.indiaembassy.net on Virtual Private Cloud (VPC) infrastructure **with data centre in India for dedicated hosting** and change the present domain name.

2.0 SCOPE OF WORK

The Service Provider shall:

2.1 Redesign, develop in Laravel platform, maintain and host Mission's multilingual website on Virtual Private Cloud (VPC) infrastructure with data centre in India for dedicated hosting;

2.2 Be responsible for provisioning of underlying system software, software licenses, infrastructure, bandwidth and Cloud Services for deployment and hosting of applications which includes hardware requirements (No. of CPU, Cores, No. of machines, RAM per machine and HDD). In no case Embassy shall pay or procure additional system/software licences..

2.3 Provision for compute, storage and bandwidth requirements which may be auto-scaled (additional capacity base on the demand and auto-scaling rules) over the period of contract in line with the transaction load to meet the requirements.

2.4 Provision for Cloud services which posses Anti Distributed Denial of Services (DDoS) feature

2.5 Carry out migration process to transfer all content from previous hosting Servers to new Cloud Servers with 7x24 hours at data centre in India;

2.6 Provide Non-Disclosure Agreement (NDA)

2.7 Comply with all 109 requirements as mentioned in **Annexure-I.**

2.8 Undertake measures to strengthen the security of the Embassy website from issues related to website vulnerabilities. Security guidelines available on the CERT-In website (www.cert-in.org.in) shall be referred and strictly complied, with regard to the following:-

(i) Web Server Security Guidelines

(ii) Guidelines for Auditing and Logging (list of empanelled auditors is also available at https://www.cert-in.org.in/PDF/Epanel.org.pdf

(iii) To ensure that website comply with the "Guidelines for Indian Government Websites (GIGW)" http://guidelines.gov.in/

2.9 Redesign/develop website which will have (i) Web 2.0 and web usability (ii) more informative about Mission and its services such as Visa, Passport, PIO and other Consular Services (iii) information about tourism, education and healthcare facilities in India (iv) information about India's history, politics, economics, foreign policies, bilateral relations between India and Myanmar (v) facility to add / modify / delete content (vi) facility to upload pictures, documents, audio and video formats (vii) search facilities within website (viii) complete administrative control to manage users with flexible access and activity controls (ix) facility to modify fonts, colours, size and layout pages (x) facility to have events (past and forthcoming events) with prior approval upon needed (xi) e-newsletter and bulk e-mail blasting (xii) facility to register online for public to get information about events and programmes of Mission; (xiii) facility to update social media.

3.0 TERMS & CONDITIONS:

3.1 Service Provider shall insure to the fullest extent possible, that Embassy of India, Yangon, Myanmar shall own any & all rights, titles & interest, including copyrights ,trademarks, trade secrets, patent & other intellectual property rights, over works created by the Service Provider.

4.0 TERMINATION

4.1. The Embassy reserves the right to terminate the contract at any time by giving 3 months advance notice. However, the Embassy shall also have the right to terminate the Contract by giving a lesser period of Notice under special circumstances, such as security considerations, violation of privacy laws, compromise of personal information, etc., and encashing the bank Guarantee for premature termination of Contract. The Service Provider may terminate the contract by giving three months advance notice with justification for termination of services. The Embassy reserves the right to impose a financial penalty in US Dollar equivalent to the service charges for one year, in case the latter terminates the contract without providing six months termination notice.

5.0 FORCE MAJORE:

5.1 The parties shall not be responsible or liable for any kind of loss whatsoever sustained by any of the parties by the extraordinary event beyond the control of the parties, such as flood, war, riots, act of God and other natural calamities which prevents one of the parties for fulfilling obligations rising out of the instant Agreement.

6.0 ARBITRATION

6.1 Neither Party, either in this agreement, or in any act related to the agreement, shall act unjustifiably or arbitrary to injure particular persons or entities or particular categories of persons or entities.

6.2 Both parties shall act in a non-arbitrary and reasonable manner with respect to the integrity of this agreement.

6.3 Any dispute, difference or question which may arise at any time hereafter between the parties relating to the true construction of this agreement or the rights and liabilities of the parties, which is not solved amicably between the parties within 30 (thirty) days, that dispute, difference or question arising shall, in the absence of agreement to the contrary between the parties, be referred to arbitration.

7.0 JURISDICTION

7.1 This Agreement shall be governed by, and construed in accordance with, Indian law in the territory 'New Delhi' only.

8.0 SIGN AND SEAL

8.1 The Bidder must sign and affix his seal on every page of the proposal and submit to Embassy.

No. YAN/ISI/305/02/2004-II

22.05.2017

TECHNICAL DETAILS TO BE PROVIDED BY THE FIRM

1	Letter of Proposal Submission.	*.pdf
2	Name, address, telephone number and e-mail of the firm	*.pdf
3	Name of responsible person for this project with mobile number and e-mail	*.pdf
4	Certificate of incorporation / Registration	*.pdf
	Proof of Annual Turn Over of last three years (certified by Chartered Accountant)	*.pdf
5	Copies of Income Tax Return of last 3 years	*.pdf
6	Certificate from any Government body that the agency has resources having domain knowledge in Web Development Governance applications. Agency needs to have documentary proof of Guidelines for Indian Government Websites (GIGW) Compliance expertise.	*.pdf
7	Previous experience for similar work (Please attaché copy of award of work from 3 different clients)	*.pdf

Signature of authroised signatory...

Name..

Company Seal & Date..

No. YAN/ISI/305/02/2004-II 22.05.2017

To
Embassy of India
Yangon, Myanmar

Subject: Proposal for Redevelopment, Upgradation and VPC web hosting of the website of the Embassy of India, Yangon

Sir,

1. We, the undersigned vendor, having read and examined in detail the Specifications and all the documents do propose to provide the Services as specified in the document No. YAN/ISI/305/2/2004-II dated 22.05.2017. We shall comply with all the 109 requirements mentioned in Annexure-I of this said document.

2. All the prices mentioned in our proposal are in accordance with the terms as specified in the documents.

3. All the prices and other terms and conditions of this proposal are valid for a period of 120 calendar days from the date of submission of proposal.

4. We, do hereby confirm that our prices include all taxes, levies etc.

5. We have carefully read and understood the terms and conditions of the and we do hereby undertake Services as per these terms and conditions.

6. We do hereby undertake that, in the event of acceptance of our proposal, the Services shall be completed as stipulated in the proposal.

Signature of authroised signatory..

Name...

Company Seal & Date...

No. YAN/ISI/305/02/2004-II 22.05.2017

Subject: Financial Proposal for Redevelopment, Upgradation and VPC web hosting of the website of the Embassy of India, Yangon

SI No.	Description	Annual Cost (US Dollar)
1	Redesign and development of existing website of Embassy as dynamic and responsive website as per SQT Certification and MEA design and technical maintenance of website	
2	Change of domain name	
3	**Hosting/shifting Charges of Website to Virtual Private Cloud Infrastructure with data centre in India**	
	TOTAL	

TOTAL IN WORDS:

Note:

1. The Financial Bid shall not include any conditions attached to it and any such conditional financial proposal shall be rejected summarily.

2. All prices should be quoted in US Dollars and indicated both in figures and words. Figures in words will prevail.

3. The cost should include all travel costs, shipping/mail, telephone/fax charges and agency administrative costs that may be incurred by the agency as part of this contract.

ANNEXURE-I

No. YAN/ISI/305/02/2004-II 22.05.2017

Subject: Proposal for Redevelopment, Upgradation and VPC web hosting of the website of the Embassy of India, Yangon

Category	S.No.	Requirement	Description
Regulatory	1	Data center locations should be in India	Cloud provider should offer cloud services from within India.
Regulatory	2	Maintain and ensure data locality	Cloud provider should ensure that customer data resides only in the Region they specify.
Regulatory	3	Protect your applications from the failure of a single location	Cloud provider should offer data centers engineered to be isolated from failures in other data centers, and to provide inexpensive, lowlatency network connectivity to other data centers in the same region.
Computer	4	Compute instances – Burstable performance	Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.
Computer	5	Compute instances – Dedicated	Cloud provider should offer instances that run on hardware dedicated to a single customer.
Computer	6	Resize virtual cores, memory, storage seamlessly	Customer must be able to specify and modify server configuration (CPU, memory, storage) parameters seamlessly and without outage.
Computer	7	Local disk/Instance	Cloud service should support local storage for compute instances to be used for temporary storage

		store	of information that changes frequently.
Computer	8	Provision multiple concurrent instances	Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.
Computer	9	Auto Scaling support	Cloud service should be able to automatically increase the number of instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
Computer	10	Bring your own image/Instance Import	Customer should be able to import their existing image and save it as a new, privately available image that can then be used to provision instances in the future.
Computer	11	Export Instance Image	Cloud service must support the ability to take an existing running instance or a copy of an instance and export the instance into a VMDK or VHD image format.
Computer	12	Instance failure recovery	Cloud service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails.
Computer	13	Instance restart flexibility	Cloud provider must be able to schedule events for customer's instances, such as a reboot, stop/start, or retirement. Depending on the event, customer might be able to take action to control the timing of the event.
Computer	14	Support for Docker containers	Cloud service should support containers, including Docker and/or other containerization platforms.
Computer	15	Highly scalable, high performance container management service	Cloud provider should offer a highly scalable, high performance container management service.

Computer	16	Event-driven computing that runs code in response to events	Cloud service should be able to run customer code in response to events and automatically manage the compute resources.
Computer	17	Pay-as-you-go pricing	Cloud provider should offer a simple pay-as-you-go pricing where customers can pay for compute capacity by the hour with no longterm commitments.
Networking	18	Multiple network interface/instance	Cloud service should be able to support multiple (primary and additional) network interfaces.
Networking	19	Multiple IP addresses/instance	Cloud service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network interface.
Networking	20	Ability to move network interfaces and IPs between instances	Cloud service should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.
Networking	21	Network traffic logging - Log traffic flows at network interfaces	Cloud service should support capturing information about the IP traffic going to and from network interfaces.
Networking	22	Auto-assigned public IP addresses	Cloud service should be able to automatically assign a public IP to the instances.
Networking	23	IP Protocol support	Cloud service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols.
Networking	24	Static public IP	Cloud provider must support IP addresses associated with a customer account, not a particular instance.

		addresses	The IP address should remain associated with the account until released explicitly.
Networking	25	Subnets within private network	Customer should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block.
Networking	26	Subnet level filtering (Network ACLs)	Cloud service should support subnet level filtering – Network ACLs that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
Networking	27	Ingress filtering	Cloud service should support adding or removing rules applicable to inbound traffic (ingress) to instances.
Networking	28	Egress filtering	Cloud service should support adding or removing rules applicable to outbound traffic (egress) originating from instances.
Networking	29	Disable source/destinati on checks on interfaces	Cloud service should support the ability to disable source/destination check on network interfaces. By default, compute instances perform source/destination checks.
Networking	30	Configure proxy server (NAT instance) at network level	Cloud service should support NAT instances that can route traffic from internal-only instances to the Internet.
Networking	31	Multiple VPN Connections per Virtual Network	Cloud service should support creating multiple VPN connections per virtual network
Networking	32	DNS based global load balancing	Cloud service should support Load balancing of instances across multiple host servers.
Networking	32	DNS based global load balancing	

Networking	33	Load balancing supports multiple routing methods	Cloud service should support multiple routing mechanism including round-robin, failover, sticky session etc.
Networking	34	Front-end Load Balancer	Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.
Networking	35	Back-end Load Balancer	Cloud service should support an internal load balancer that routes traffic to instances within private subnets.
Networking	36	Health checks - monitor the health and performance of application	Cloud service should support health checks to monitor the health and performance of resources.
Networking	37	Integration with Load Balancer	Cloud service should support integration with load balancer.
Networking	38	Low Latency	The CSP should be able to provide a 10GB network connectivity between the servers if required.
Storage – Block Storage	39	Support for storage allocated as local disk to a single VM	Cloud provider should offer persistent block level storage volumes for use with compute instances.
Storage – Block Storage	40	Storage volumes > 1 TB	Cloud provider should offer block storage volumes greater than 1 TB in size.
Storage – Block Storage	41	SSD backed storage media	Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies.

Storage – Block Storage	42	Provisioned I/O support	Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
Storage – Block Storage	43	Encryption using provider managed keys	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
Storage – Block Storage	44	Encryption using customer managed keys	Cloud service should support encryption using customer managed keys.
Storage – Block Storage	45	Durable snapshots	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.
Storage – Block Storage	46	Ability to easily share snapshots globally	Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data center migration, and disaster recovery.
Storage – Block Storage	47	Attach more than one compute instance to a single volume	Cloud service should support adding more than one compute instance to a single storage volume in R/W mode so that many users can access and share a common data source.
Storage – Block Storage	48	Consistent Input Output per second (IOPS)	Cloud service should support a baseline IOPS/GB and maintain it consistently at scale
Storage – Block Storage	49	Annual Failure Rates <1%	Cloud service should be durable and support annual failure rates of less than 1%
Storage – File Storage	50	Simple, scalable file storage service	Cloud provider should offer a simple scalable file storage service to use with compute instances in the cloud.

Storage – File Storage	51	SSD backed storage media	Cloud service should offer SSD backed storage media to provide the
Storage – File Storage			throughput, IOPS, and low latency needed for a broad range of workloads.
Storage – File Storage	52	Grow file systems to petabyte scale	Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections.
Storage – File Storage	53	Consistent low latency performance (T50-T99)	Cloud service should support consistent low latency performance between 5-15 ms at any scale.
Storage – File Storage	54	Scalable IOPS and throughput performance (/TB)	Cloud service should support scalable IOPS and throughput performance at any scale.
Storage – File Storage	55	Sharable across thousands of instances	Cloud service should support thousands of instances so that many users can access and share a common data source.
Storage – File Storage	56	Fully elastic capacity (no need to provision)	Cloud service should automatically scale up or down as files are added or removed without disrupting applications.
Storage – File Storage	57	Highly durable	Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple data centers.
Storage – File Storage	58	Read-after-write consistency	Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).
Relational Database	59	Managed relational database	Cloud provider should offer a service that makes it easy to set up, operate, and scale a relational

		service	database in the cloud.
Relational Database	60	Support for MySQL	Cloud service should support the last two major releases of MySQL (versions 5.6, 5.5) as a database engine.
Relational Database	61	Support for Oracle	Cloud service should support the last two major releases of Oracle (11g and 12c) as a database engine.
Relational Database	62	Support for Microsoft SQL Server	Cloud service should support all the editions (Express, Web, Standard, Enterprise) of SQL Server 2012 as a database engine.
Relational Database	63	Support for PostgreSQL	Cloud service should support the last two major releases of PostgreSQL (9.4.x, 9.3.x)
Relational Database	64	Low latency, synchronous replication across multiple data centers in a region	Cloud service should support synchronous replication of a primary database to a standby replica in a separate physical datacenter to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
Relational Database	65	Read Replica support	Cloud service should support read replicas that make it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads.
Relational Database	66	Manual Failover	Cloud service should support a manual failover of the DB instance from primary to a standby replica.
Relational Database	67	Provisioned IO support	Cloud service should support the needs of database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
Relational Database	68	Bring your own SQL, Oracle licenses	Cloud service should support customers who prefer to use their existing Oracle and SQL Server database licenses in the cloud.

Relational Database	69	Cross region Snapshots	Cloud service should support copying snapshots of any size between different cloud provider regions for disaster recovery purposes.
Relational Database	70	Cross region Read Replica	Cloud service should support creating multiple in-region and crossregion replicas per database instance for scalability or disaster recovery purposes.
Relational Database	71	High Availability	Cloud Service should support enhanced availability and durability for database instances for production workloads.
Relational Database	72	Point in time restore	Cloud service should support restoring a DB instance to a specific date and time.
Relational Database	73	User snapshots and restore	Cloud service should support creating a DB snapshot and restoring a DB instance from a snapshot.
Relational Database	74	Modifiable DB parameters	Cloud service should allow the DB parameter to be modified.
Relational Database	75	Monitoring	Cloud service should allow monitoring of performance and health of a database or a DB instance.
Relational Database	76	Encryption at rest	Cloud service should support encryption using the industry standard AES-256 encryption algorithm to encrypt data.
Security and administratio n	77	Control access to your cloud resources at a granular level	Cloud provider should offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device.
Security and administratio n	78	Utilize multi-factor	Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.

Security and administration	78	authentication when accessing cloud resources	Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.
Security and administration	79	Identify when an access key was last used to rotate old keys and remove inactive users	Cloud service should support reporting a user's access keys last use details.
Security and administration	80	Policy Simulator to test policies	Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production.
Security and administration	80	before committing to production	Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production.
Security and administration	81	Policy validation to ensure policies match intentions	Cloud service should support a policy validator to automatically examine non-compliant access control policies.
Security and administration	82	Directory as a service	Cloud provider should support setting up a stand-alone directory in the cloud or connecting cloud resources with existing on-premises Microsoft Active Directory.
Security and administration	83	User and Group management	Cloud service should support features such as user and group management.
Security and administration	84	Managed service to create and control the encryption keys used to encrypt	Cloud provider should offer a service to create and control the encryption keys used to encrypt user data.

		your data	
Security and administration	85	Audit of all action on keys	Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.
Security and administration	86	Key Durability	Cloud service should support durability of keys, including storing multiple copies to ensure keys are available when needed.
Security and administration	87	Durable and inexpensive log file storage	Cloud service should support storing log files in a durable and inexpensive storage solution.
Security and administration	88	Choice of partner solution	Cloud service should support a variety of 3rd party solutions.
Security and administration	89	Automatically records a resource's configuration when it changes	Cloud service should automatically record a resource configuration when it changes and make this information available.
Security and administration	90	Examine the configuration of your resources at any single point in the past	Customer should be able to obtain details of what a resource's configuration looked like at any point in the past using this cloud service.
Security and administration	91	Receive notification of a configuration change	Cloud service should notify every configuration change so customers can process these notifications programmatically.
Security and administration	92	Create and manage catalog of pre-approved services for use	Cloud provider should offer the ability to create and manage catalogs of IT services that are approved for use.

Deployment and Management	93	Service to quickly deploy and manage applications in the cloud	Cloud provider should offer a service to quickly deploy and manage applications in the cloud by automatically handling the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.
Deployment and Management	94	Supported OS	Cloud Service should support Windows, Linux, and Docker containers.
Deployment and Management	95	Deployment Mechanism	Cloud service should support various deployment mechanisms, including a Git repository, or an integrated development environment (IDE) such as Eclipse or Visual Studio.
Deployment and Management	96	Support for SSL connections	Cloud service should support SSL connections.
Deployment and Management	97	Auto scaling	Cloud service should support automatically launching or terminating instances based on the parameters such as CPU utilization defined by users.
Deployment and Management	98	Swap virtual IP between staging and production environments	Cloud service should support swapping IP addresses between staging and production environments so that a new application version can be deployed with zero downtime.
Deployment and Management	99	Integration with caching solution	Cloud service should be integrated with a caching solution such as Redis cache.
Deployment and Management	100	Service to create a collection of related resources and provision them using a template	Cloud provider should offer a service to create a collection of related resources and provision them in an orderly and predictable fashion using a template.

Deployment and Management	101	Single JSON based template to declare your stack	Cloud service should use a template, a JSON-format, text-based file that describes all the resources required for an application. The resources in the template should be managed as a single unit.
Deployment and Management	102	Allow parametrization and specific configurations	Cloud service should support parameterization for specific configuration.
Deployment and Management	103	Integration with the portal	Cloud service should be integrated with the portal.
Support	104	Service Health Dashboard	Cloud provider should offer a dashboard that displays up-to-theminute information on service availability across multiple regions.
Support	105	365 day service health dashboard and SLA history	Cloud provider should offer 365 days' worth of Service Health Dashboard (SHD) history.
Support	106	Service to compare resource usage to best practices	Cloud provider should offer a service acts like a customized cloud expert and helps provision resources by following best practices.
Support	107	Monitoring Tools	Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health.
Support	108	Governance and Compliance	Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines. Ability to choose from a set of pre-built rules based on common best practices or custom rules (e.g., ensure Storage

			volumes are encrypted, Compute instances are properly tagged, and Elastic IP addresses (EIPs) are attached to instances) and continuously monitor configuration changes to the cloud resources and provides a new dashboard to track compliance status.
Support	109	Audit Trail	Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing

—o—