

## **Alliance & End AIDS India Website Hosting**

### **About Alliance India**

Founded in 1999, Alliance India is a non-governmental organisation operating in partnership with civil society, government and communities to support sustained responses to HIV in India that protect rights and improve health. Complementing the Indian national programme, we build capacity, provide technical support and advocate to strengthen the delivery of effective, innovative, community-based HIV programmes to vulnerable populations affected by the epidemic.

**This RFP is floated to select the agency to host Alliance India and End AIDS India Website and Server.**

### **Data Centre to Host Alliance India's Server.**

- As per Alliance India requirement data centre should be within India.
- The vendor will be required to deal with highly sensitive data regarding the key population.
- The agency should guarantee the confidentiality of the data kept in the server and should be ready to sign an unconditional non-disclosure agreement with Alliance India in the event of their selection.

**The required specifications/configurations of the data centre:**

#### **1. Roles and Responsibilities**

- Server and Network management, administration, and maintenance.
- Manage Servers from the infrastructure level i.e., Compute and Storage.
- Provide remote data backup for servers.
- The disaster recovery/redundancy plan proposing for the Alliance Server by the agency
- Monitor and install Patches and Updates for Servers and networked computers on a demand basis.
- Install and maintain antivirus and malware protection.
- Help desk Support.
- Any other necessary service/services to maintain a stable and safe I.T. infrastructure.

#### **2. Infrastructure:**

The vendor to guarantee that the critical infrastructure systems, including power and HVAC, will be available 100%, excluding scheduled maintenance.

#### **3. Hardware Guarantee:**

The vendor to provide the network guarantee with the functioning of all hardware components and will replace any failed component at no cost to the customer.

#### **4. Network Uptime:**

The vendor to provide the network guarantee that the network Uptime, including Internet connectivity and availability of network switch and hardware servers, will be available 100%, excluding scheduled maintenance.

#### **5. Uptime**

It shall be the responsibility of the vendor to provide an uptime of not less than 99.90%. This uptime includes the following on the part of the service provider:

- Network uptime at the datacentre where our server is hosted.
- Mail services receiving and sending of mails should be possible at all times using POP3 as well as HTTP access as applicable.
- Hardware and other infrastructure facilities maintained by the service provider at their datacentre.

#### **6. Server maintenance**

The vendor should be upgrading Latest Security Patches, Upgrading Latest Software Modifications as they are announced. This typically happens during off-hours and part of routine administrative maintenance.

**7. 24&7 hours Server monitoring**

We want our servers to be constantly monitored by special monitoring software. If a server goes down for some reason, the system automatically logs the same.

**8. Server Hardware Configuration.**

S. No.	OS	vCPUS	RAM	SSD	Backup	Bandwidth	DB
1	Red Hat or Cent OS & WHM with License	4	16	1 TB	1 TB	Unlimited	My SQL license Included
2	Red Hat or Cent OS & WHM with License	8	16	1 TB	1 TB	Unlimited	My SQL license Included
3	Web Site & DB – Backup					Included	

**9. Detailed SLA with standard escalation matrix can be referred to with the attached SLA File.**

**9.1 Escalation Matrix**

Incident Classification			
Alert	Description	Response Time	Resolution Time
Severity 1	System Down, significantly affecting End Customers	Immediate	2 Hrs.
Severity 2	System performance severely degraded but still functioning	10 Min	4 Hrs.
Severity 3	Error not significantly affecting End Customers /Users	15 Min	6 Hrs.
Severity 4	Service request	30 Min	12 Hrs.
Change Request	Description	1 Hrs.	TBD

**10. Physical Security should meet the below-mentioned requirements:**

Data centre point of view physical security should include below mentioned things.

**10.1 . Secured physical access to data centres which comprises of: -**

- Single access point of control
- Biometric devices
- Smart card access
- Body scanner
- Goods X-Ray

**10.2. Infrastructure comprises of: -**

- Secure cages and racks
- Fire protection
- Water Proofing
- Anti-Rodent Devices

**Power Management:**

- 24& 7 Power supply

**10.3. Network security includes: -**

- Network planning
- BGP (Border Gateway Protocol)
- Firewalls

- Core Routers and Switches

**Logical Security Should meet the below-mentioned requirements.**

- Access permissions for authorized access
- Encrypt Data Communication using: -
  - SSH
  - SFTP
  - SSL VPN and VPN site to site connections
- Keep OS and Software Up to Date
- User Accounts and Strong Password Policy
- Implement a firewall for an additional layer of security.
- Disable Unwanted Services through port blocking, firewall rules and policy implementation.
- Logging and Auditing through monitoring & alert tools
- Intrusion Detection and Prevention System
- Backups
- Antivirus, Antimalware, Antispyware.

**11. Disaster Recovery:**

- The vendor requires 100% availability. Any failures to meet this target must result in penalties payable as per predetermined penalty clauses.
- The datacentre must be connected to one or more additional data centres situated in India and the data replicated every 15 minutes from the primary to the secondary data centre.
- Disaster recovery tests of Vihaan hosted servers and applications must be conducted every six months by the service provider and the results reported to Alliance India.
- Downtime Response – There must be a system where the moment the website is down designated people in Alliance India must get a communication.

**Data ownership**

- All data stored by the system is solely owned by Alliance India and should be always accessible.

**12. Back up requirements:**

The service provider must provide a backup service for Alliance India data located in the service provider's data centre that meets the requirements listed below.

**13.1. Backup schedule**

Server	Backup Plan	ITEMS TO BACK UP	SCHEDULE	HOW MANY TO KEEP
Server 1	Image	Entire machine	Incremental: Every day Full: 1 of each month	30 Days
	MYSQL	My SQL data	Incremental: Every day Full: 1, 16 of each month	30 Days
Server 2	Image	Entire machine	Incremental: Every day Full: 2, of each month	30 Days
	MySQL SERVER	My SQL data	Incremental: Every day Full: 2, 17 of each month	30 Days

