DEPARTMENT OF TAXES
OFFICE OF THE COMMISSIONER OF TAXES
NAGALAND: DIMAPUR

e - mail ID: cotgon@rediffmail.com

Corrigendum - 1 to the RFP No. CT/MMP-CT/NIC/17/10/CONTD. Dated 21.01.2012 for the for Supply Installation Commissioning Operation & Maintenance of Hardware and Networking Equipments

Date of Issuance: 23.02.2012

Annexure-4 Bill of Material

Component		Total Qty.
A	COMPUTING HARDWARE	
1	Database Server	2
2	Application Server	2
3	Backup Server	2
4	Anti Virus Server	1
5	Client Type - I / Desktops	163
6	Laptops	11
7	Laser Printers	53
8	DMP	20
9	Scanner	20
B	NETWORKING HARDWARE	
1	Router I	3
2	Router II	12
3	Switch-24 Port	26
4	Server Racks (42U)	2

5	Wall Mount Rack (9U)	26
6	Firewall and Intrusion Detection & Prevention System	1
7	NMS and SLA Monitoring Software	1
C	POWER REQUIREMENTS	
1	UPS 10 KVA	12
2	UPS 5 KVA	6
D	SYSTEM SOFTWARE REQUIREMENTS	
1	O/S for Server	7
2	RDBMS (SQL Server 2008 Enterprise Ed.)	2
3	AV Server	1
4	Anti Virus Client	174
5	MS Office Suite	174
E	LAN REQUIREMENTS	
2	24 Port CAT6 UTP Jack Panel with Cable Manager	26
3	Cat 6 Cable - 305 Mtr	30
4	Face Plate (SINGLE)	174
6	Single Information Outlet with SMB having shutter facilty	174
8	Back Box	174
9	Patch Cord 1 Mtr	174
10	Patch Cord 2 Mtr	174

1. Specification of Firewall

Hardware features

§ The Firewalls should be Hardware based, Reliable, purpose -built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems with 6 No's of 10/100/1000 Base TX interfaces

- § The Appliance should be Full -featured, high-performance firewall and IP Security (IPSEC) VPN technologies deliver robust application security, user- and application-based access control, and remote User/site connectivity.
- § Should be redundant supporting Active/Active or Active/Standby Firewall for Availability & Scalability
- § Should have Adequate memory DRAM/Flash
- § Firewall Throughput of 1 GBPS for 64 byte packets
- § Encrypted Throughput : minimum 400 Mbps
- § Concurrent connections of up to 400,000
- § simultaneous VPN tunnels 2000
- § Support for Virtual Firewalls of at least 50 logical firewalls so that the Central site can have individual firewalling for every remote site in future
- § Virtual Interfaces (VLANs) support for at least 100 VLANs for forming Secure Server Farms and DMZs
- § Scalability through VPN clustering and load balancing.
- § Should have Active & failover on state full & LAN based.

IOS Features

- § Application Security Services Support
- § The Firewall should have Integrated specialized inspection engines for protocols Like HTTP, FTP, ESMTP, DNS, SNMP, ICMP, SQL*Net, NFS, H.323 Versions 1 -4, SIP, MGCP, RTSP and TAPI over CTIQBE protocol, GTP, LDAP, ILS, RPC and many more.
- § The Firewall should provide advanced inspection services to detect and Block instant messaging, peer-to-peer file sharing, and other applications tunneling through Web application ports.
- § Advanced H.323 inspection services to provide flexible security integration in a variety of H.323-driven voice-over-IP (VoIP) environments
- § Fortified SIP inspection engine that secures both, UDP and TCP based SIP environments.
- § NAT- and PAT-based address translation support for SIP -based IP phones and applications as Microsoft Windows Messenger, while delivering advanced services such as call forwarding, call transfers, and more Secure integration of IP telephony services while connecting calls over multiprotocol VoIP environments across NAT and PAT boundaries

- Rich MGCP security services and NAT- and PAT-based address translation services for MGCP-based connections between media gateways and call agents or media gateway controllers.
- Support for IPSEC site to site VPN & client to site VPN has to be there for unlimited Peers.

Support for Network Containment and Control Services

- Robust stateful inspection firewall services that track the state of all network Communication.
- Inbound and outbound access control lists (ACLs) for interfaces, and per -user or - group policies for improved control over network and application usage.
- Support for High-Availability Service
- Support for Active/Active & Active/Standby failover.
- Support for bidirectional state sharing between Active/Active failover pair members for support of advanced network environments with asymmetric routing topologies, allowing flows to enter through one Firewall appliance and exit through the other, if required
- Maximizing VPN connection uptime with Active/Standby stateful failover for VPN Connections.
- Support for Synchronizing all security association state information and session key material between failover pair members, providing a highly resilient VPN solution.
- Enable geographic separation of Security appliances in a failover pair by allowing failover information to be shared over a dedicated LAN connection between pair members
- Support to perform software maintenance release upgrades on the Firewall appliance failover pairs without affecting network uptime or connections.
- Enable creation of multiple security contexts (virtual firewalls) within a single appliance, with each context having its own set of security policies, interfaces, and administrative domains
- Support for 50 number of virtual firewalls on the same hardware firewall. Providing a convenient way of consolidating multiple firewalls into a single physical appliance or failover pair, while retaining the ability to separately manage each of these virtual instances.
- Support for multiple virtual interfaces on a single physical interface through VLAN trunking and multiple VLAN trunks per appliance
- Comprehensive OSPF dynamic routing services. Improved network reliability fast route convergence and secure, efficient route distribution. Secure routing solution in environments using NAT through tight integration with NAT services.
- Delivery of multimedia traffic in videoconferencing, collaborative computing, and Mission-critical real-time enterprise applications through full PIM Sparse Mode v2

- Facilitate a wide range of multicast applications by including support for Internet Group Management Protocol (IGMPv2) and stub multicast routing, including NAT and PAT and the ability to build ACLs for multicast traffic

- Should be able to mark the packets based on the defined policies so that the flows can be treated at the router

- Access control and deep inspection firewall services for native IPv6 network environments and mixed IPv4 and IPv6 network environments through dual - stack support

- IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and Support for SSHv2, Telnet, HTTP and HTTPS

2. Technical Specification of Intrusion Prevention system, Active & Failover

General Features:

- Should be chassis based with minimum 1Gbps throughput
- Redundancy should be keep in mind the requirement is for Active & standby Unit with auto failover with all running rules & configuration.
- Having the capability to run in LAN mode and Promiscuous mode.
- Content-based:
- IPS should have the capability to inspect the content of network packets for unique sequences, called signatures, to detect and hopefully prevent known types of attack such as worm infections and hacks.

Protocol Analysis

- The key development in IPS technologies is the use of protocol analyzers. Protocol analyzers should natively decode application-layer network protocols, like HTTP or FTP. Once the protocols are fully decoded, the IPS analysis engine should evaluate different parts of the protocol for anomalous behavior or exploits.
- IPS engines should be fully protocol analyzers. The IPS should be placed just before the gateway of the Internet & it will sync with internet to update latest signature file. Should have the capability to protect the internal zone from any shorts of attack including Denial service, IP flooding, hacking & should able have the capability to generate customize report hourly , weekly, monthly & yearly reports. Reports & alarms should be floated by the e mail service to the respected people.
- Rate-based
- IPS should be primarily intended to prevent DoS and DDoS attacks. The work by monitoring and learning normal network behaviors. Through real-time traffic monitoring and comparison with stored statistics, IPS should identify abnormal rates for certain types of traffic e.g. TCP, UDP or ARP packets, connections per second, packets per connection, packets to specific ports etc. Attacks are detected when thresholds are exceeded. The thresholds are dynamically adjusted based on time of day, day of the week etc., drawing on stored traffic statistics.
- Unusual but legitimate network traffic patterns may create false alarms. The system's effectiveness is related to the granularity of the RBIPS rule base and the quality of the stored statistics.

Once an attack is detected, various prevention techniques may be used such as rate-limiting specific attack-related traffic types, source or connection tracking, and source-address, port or protocol filtering (black-listing) or validation (white-listing)

3. Scanner

Features	Specifications
scanner type	Flatbed
input modes	front panel scan, copy buttons,
speed	**preview speed:** 10 seconds **Scan speed:** Photo to files: 29 secs; Text to document: 26 secs
resolution	4800 dpi optical resolution, 4800 x 9600 dpi hardware resolution,
imaging technology	CCD
bit depth	48-bit
scaling	10 to 2000%
max document size	220 x 300 mm
interface and operating system requirements	USB – compatible with USB 2.0 Windows XP Home and Professional Edition ; Windows 7 Professional; Linux
power	Universal AC adaptor: 100 to 240 VAC (+/- 10%), 50/60 Hz (+/- 3Hz) input (according to configuration), 12 VDC, 1.25 Amp output, Energy Star™ compliant

4. Antivirus Software

Anti Virus software to protect LAN Servers

The software should be with following functionality:

- Shall provide domain based central management – organize and manage computers in logical domains
- Shall support pattern file rollback – shall be able to return to past pattern file if problem with new file
- Shall be able to scan through minimum of 19 types of compression formats and shall be able to scan through 20 levels of compression
- Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
- The solution should support true file type or true file type group scanning and blocking
- Shall be able to remotely uninstall the antivirus software
- Shall support the following platforms: Windows NT/2000 (x86), Netware, Linux (real- time scan), EMC Celerra & NetApp Filer
- The solution shall be able to block specified ports and Network shares on all the servers to stop the proliferation of Network viruses which use ports to spread after entering the Network
- Shall be certified by the following vendors & products:
  - Microsoft Windows 2000 Server, Advanced Server & Datacenter Server
  - Citrix Metaframe Server
  - IBM xSeries Server
  - HP/Compaq Datacenter Server
- System does not require restarting of the Virus Scanning service after a Pattern update
- Shall be able to scan Object Linking and Embedding (OLE) File
- Anti Virus software to protect Desktops on the network
- The software should be with following functionality:
- Must have a Personal Firewall to protect the clients from common network based hacker attacks and Intrusion detection features
- Must have enhanced Spyware/Adware detection capabilities in real-time
- Must have exclusion list to exclude Spyware/Adware from scanning
- Virus Outbreak Monitor and Firewall Outbreak Monitor to notify the Antivirus server/Administrator when the client detects excessive network traffic or log counts from IDS/personal firewall exceed certain thresholds respectively
- Should have flexible port blocking capabilities in the Personal Firewall component which can permit or deny traffic from a specified port or range of ports
- The Client firewall should use stateful inspection to scan network traffic for profile and security level; filters connections by IP address, port number and protocol
- Should support Network Virus Scanning to detect and drop infected packets from the network layer
- Must integrate with Checkpoint VPN 1 SecureClient to ensure that all Remote clients connecting via a VPN comply with the company's antivirus policy
- Outbreak Prevention option to block specific shared folders, ports, and to deny write access to specified files and folders on selected clients from the central console during a virus outbreak
- Should be able to specify CPU usage during file scans

- Should have a feature to consolidate virus logs resulting from recurring infections made by the same network virus and send them to the Antivirus server
- Should provide Comprehensive Support for Network Admission Control
- Should be able to deploy the Admission Control Agent along with the antivirus client deployment
- Should come in-built with a Policy server which will have the ability to configure settings to perform actions on at-risk clients to bring them into compliance with the organization's antivirus policies
- Should be able to deploy the Client software using the following mechanisms:
  - Support MSI in Client Packager tool
  - Notify Clients to install via E-Mail
  - Client Packager tool for client local install
  - Web Install via Active X control
  - NT Remote Install
  - Via Login Script
  - Through disk imaging
  - Support MS Systems Management Server (SMS)
- There should be only a one-time deployment of the client Antivirus components (Antivirus, Firewall, Spyware and Damage Cleanup) rather than deploying it separately
- The update component should download all components required including the pattern file, scan engine, program files, damage cleanup template/engine, Spyware pattern, firewall engine and network worm engine instead of downloading every component separately
- The Server component should have the flexibility to update itself from multiple update sources
- Clients should get virus updates, Spyware/Adware pattern updates, network worm updates and personal firewall updates from a single server Antivirus server
- Clients should automatically look at another update source to get updates if the primary antivirus server is not available
- Solution must allow specified clients to act as Update Agents (sources for updated components) so other clients can receive updates from these clients to ensure effective use of corporate bandwidth
- Should provide with Web-based centralized management through which all the clients can be centrally managed / configured for antivirus and firewall policies
- Secure remote access via Web browser (SSL-enabled)
- Should have an integrated feature to backup the client's database
- Customizable client alert message for virus detection and Personal Firewall
- Should generate Virus activity log, update log, Personal firewall/intrusion detection log, network virus logs, Client connection status log and Server system event log and should be able to send notification to the infection source
- A quarantine manager to set the capacity of the quarantine folder and the maximum size of the quarantined files
- Should have a feature to scan and detect for vulnerable systems in the network and remotely deploy the client software to them automatically
- Able to automatically uninstall existing antivirus software at the desktop
- Should have an option to reserve specified amount of space on the client only for updates
- Solution should be capable of protecting itself from virus attacks
- Protect the Operating Systems i.e. Windows / Linux/Unix

HTTP Gateway level Antivirus and URL Filtering solution

- The solution should be a single product solution to provide HTTP & FTP Gateway level Antivirus. The product should be software based solution

- The solution should support Microsoft Windows & Linux platforms
- The solution should be a fully integrated solution designed to block Web-based threats, including Viruses, Trojans, Worms, Phishing attacks and Spywares / Adwares
- The solution should be capable of preventing installed Spyware from sending confidential data via HTTP
- The solution should be capable of working in the following configurations:
  - As a standalone proxy,
  - Integrated with upstream proxy servers
  - Integrated with ICAP-compliant caching servers, Network Appliance, or BlueCoat,
  - It should be capable of working as a transparent proxy utilizing WCCP or a Load balancer
  - Reverse proxy
- The solution should support True File type scanning
- The solution should be capable of automatically blocking Infected URLs
- The solution should be capable to taking action on password-protected or encrypted files
- The solution should Encrypt the Quarantined files
- The solution should have the following options for handling large files: Scan first, Deferred Scan and Scan behind
- The solution should be able to selectively bypass certain MIME content types
- The solution should be capable of automatically sending a customized email message on detecting malicious code in a file, which a user requested
- The solution should be able to define Scan limits for compressed files based on the following criteria: Number of files inside the compressed file, Decompressed file size, Decompression percentage and decompression layers
- The solution should have Inbuilt logging and reporting capabilities (Reports by User/Group, Consolidated user reports, Blocking events report, traffic report etc.)
- The solution should log performance statistics, including CPU usage, Memory usage, and number of transactions processed
- The solution should support for Remote Installation
- The solution should support SNMP based System and Event Notifications
- The solution should have the capability to control access to the IWSS server based on IP addresses
- The solution should be able to Rollback the pattern file update if required
- It should allow setting of URL policies by category, group, or user and control access by time of day, day of week, and bandwidth quotas to improve network performance, reduce legal liability, and increase productivity
- It should support Microsoft Active Directory, Linux OpenLDAP Directory and Sun Java System Directory Server via LDAP, enabling IT administrator to easily set policies and assign rules for single PCs or groups
- Support for Customizable URL access/deny Rule Sets and additional customizable allow/deny categories & Sites
- URL, Internet resource access restriction capability based on Network, IP Address, Users, Groups etc.
- SMTP/POP3 Gateway Level Anti Virus and Anti Spam Solution
- The solution should be a single product integrated solution to provide SMTP/POP3 Antivirus, Content Filtering and Heuristics based Anti Spam Solution. The product should be software based solution
- The solution should work on Windows & Linux Platforms
- The solution must support
  - mass mailing virus detection

  - mail attachment virus detection
  - malformed Mail format detection
- The solution should provide heuristic evaluation of compressed files that helps reduce the risk that a virus compressed using these methods will enter your network via email
- The solution must have a built in Safe Stamp feature
- The solution must have its own Updated Recommended Virus Extensions
- The solution must support at least 20 types of Compression algorithms
- The solution must support Heuristics-based mail header detection for Spam and scanning of the mail body for Spam
- The solution must support administrator defined Anti-Spam exception list (white list) or administrator-defined blacklists of known spammers
- The solution should be able to detect Spam based on multiple categories (such as general, commercial email, Get rich quick, pornography, Racially insensitive content) and take action based on the category in which Spam is detected
- The solution should provide End User Quarantine (EUQ) feature with Web-based end user access to spam quarantines
- The solution must be able to take different action based on the different sensitivity level of Spam detection
- The solution must support Keyword search in message body and Intelligent Keyword Search (NEAR, NOT, WILD, OCCUR N times operators)
- The solution must be able to scan by message subject, header, body, and attachment objects and must be able to strip off attachments
- The solution must support Attachment Filtering based on file name and extension
- The solution must support Attachment Filtering based on real/true file type (file header based checking)
- The solution must support Attachment Filtering based on number of attachments
- The solution must be able to block message by mail size and attachment size
- The solution must have its own Spam signature database that should be updated automatically
- The solution must have the ability to add legal disclaimers to the message
- The solution must be able to postpone sending of over size message
- The solution must support
  - Email archiving
  - Recursive Analysis on message and compressed files.
  - Encoding Formats MIME, UUENCODE, MS-TNEF, BINHEX
- The solution should have a built-in watchdog agent monitors the health of the solution and delivers notifications through email or SNMP trap when a fault condition threatens to disrupt the mail flow
- The solution should provide centralized spam reporting

Management of Anti-Virus deployment

- Shall manage the anti-virus programs on the network from a single web-based console
- Shall provide network wide virus statistics and analysis
- Must be able to do centralized update to all anti-virus programs on the network
- It shall be able to monitor remote locations over WAN links for anti virus activity
- Shall provide Incident monitoring and notification
- System reporting shall provide Information collected throughout network for analysis of activity; graphical report generation
- Shall eliminate the need for platform-specific computer skills when administering the variety of anti-virus programs often found on the network

- Shall be interactive and event-driven communication minimizes network traffic
- Shall allow administrators to enforce an enterprise-wide virus protection policy from one GUI monitor
- Shall support 3-tier deployment architecture to have better bandwidth management. Example, Parent Management console -> Child Management Console -> Managed Anti-Virus Products
- Shall provide proactive attack process management, focused on getting attack specific information and policy file to IT administrators before new pattern file available
- Shall be able to perform all necessary outbreak related tasks from a single interface

Shall offer a hierarchical structure for job delegation so administrators can determine access control.

The management system's users shall be classified into Administrator, Power User or Operator roles

TECHNICAL SPECIFICATION OF NMS AND SLA MONITORING SOFTWARE

Basic Requirements

- Solution should be inclusive with hardware, OS, patches, etc.
- Bidder should provide a centralized Management solution for all the IT assets spread across various units.
- Should be SNMP v1, v2, v3 and MIB-II compliant.
- Should support Web / Administration Interface.
- Should provide compatibility to standard RDBMS.
- Solution should be open, distributed, and scalable and open to third party integration.
- Should provide fault and performance management for multi-vendor TCP/IP networks.

Polling Cycle

- Support discriminated polling
- Should be able to update device configuration changes such as re-indexing of ports

Fault Management

- Should be able to get fault information in real time and present the same in alarm window with description, affected component, time stamp etc.
- Should be able to get fault information from heterogeneous devices — routers, switches, servers etc.
- Event related to servers should go to a common enterprise event console where a set of automated tasks can be defined based on the policy.
- Should have ability to correlate events across the entire infrastructure components
- Should provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.
- The tool shall integrate network, server and desktop performance information and alarms in a single console and provide a unified reporting interface for network and system components. The current performance state of the entire network and system infrastructure shall be visible in an integrated console.

- Should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports

Agents

- Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agents on the servers to be monitored.
- Provide performance threshold configuration for all the agents to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents could then dynamically reconfigure them to use these threshold profiles they receive.

System Monitoring

- Should be able to monitor/manage large heterogeneous systems environment continuously.
- Windows OS
    - Should monitor / manage following:
        - Event log monitoring
        - Virtual and physical memory statistics
        - Paging and swap statistics
        - Operating system
        - Memory
        - Logical disk
        - Physical disk
        - Process
        - Processor
        - Paging file
        - IP statistics
        - ICMP statistics
        - Network interface traffic
        - Cache

        - Ø Active Directory Services
    - o Should be capable of view/start/stop the services on windows servers

Availability Reports

- Availability and Uptime – Daily, Weekly, Monthly and Yearly Basis
- Trend Report
- Custom report
- MTBF and MTTR reports

Performance Reports

- Device Performance – CPU and Memory utilized
- Interface errors
- Server and Infrastructure service statistics
- Trend report based on Historical Information
- Custom report
- SLA Reporting
- Computation of SLA for entire DC/DR Infrastructure
- Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports

Integration

- Should be able to receive and process SNMP traps from infrastructure components such as router, switch, servers etc.
- Should be able integrate with Helpdesk system for incidents.
- Should be able to send e-mail or Mobile –SMS to pre-defined users for predefined faults.
- Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.

Network Management

- The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.

- It should proactively analyze problems to improve network performance.

- The Network Management function should create a graphical display of all discovered resources.

- The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display

- The Network Management function should collect and analyze the data.

- The Network Management function should also provide information on performance of Ethernet segments, WAN links and routers.

- Alerts should be shown on the Event Management map when thresholds are exceeded.

- It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.

- The Systems and Distributed Monitoring (Operating Systems) of EMS should be able to monitor:

    - Processors: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds.

    - File Systems: Each file system should be monitored for the amount of file system space used, which is compared to user-defined warning and critical thresholds.

    - Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem and in applications. The function should also analyze the files residing on the host for specified string patterns.

    - System Processes: The System Management function should provide real-time collection of data from all system processes. This should identify whether or not an important process has stopped unexpectedly. Critical processes should be automatically restarted using the System Management function.

    - Memory: The System Management function should monitor memory utilization and available swap space.

    - Event Log: User-defined events in the security, system, and application event logs must be monitored.

SLA Monitoring

- The SLA Monitoring function of the EMS is by far the most important requirement of the DC/DR Project. The SLA Monitoring component of EMS will have to possess the following capabilities:
  - EMS should integrate with the application software component of portal software that measures performance of system against the following SLA parameters:
    - Uptime of Desktop;
    - Uptime of Server
    - Uptime of Networking Components
  - EMS should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a quarter, and compare it with the SLA metrics laid down in the RFP.
  - The SLA monitoring component of the EMS should be under the control of the authority that is nominated to the mutual agreement of Director, the partner so as to ensure that it is in a trusted environment.
  - The SLA monitoring component of the EMS should be subject to random third party audit to vouchsafe its accuracy, reliability and integrity.

Annexure 23 - Breakup of Cost format

Overall Cost Break up

S.No	Phase	Total Cost (INR)
1	Computing Hardware Cost	
2	Networking Hardware Cost	
3	System Software Cost	
4	Power requirements Cost	
5	Manpower Cost	
6	Implementation Cost	
7	Other Project Related Costs	

Procurement of Hardware and Networking equipment

All hardware and network equipment procured should be in line with the specification mentioned in Annexure 2. Tenderer should provide the total amount, tax and unit price in Indian Rupee.

i) Computing Hardware

SNo.	Item	Unit Price (P)	Tax (t)	Total amount T=(P+t)	Total Qty (Q)	Total amount T*Q	Remarks
				COMPUTING HARDWARE			
1	Database Server						
2	Application Server						
3	Backup Server						
4	Anti Virus Server						
5	Desktops						
6	Laptops						

7	Laser Printers						
8	Scanner						
9	DMP						
10	Any other (Please Specify)						
	INR 0.00						

ii) Networking Hardware

SNo.	Item	Unit Price (P)	Tax (t)	Total amount T=(P+t)	Total Qty (Q)	Total amount T*Q	Remarks
NETWORKING HARDWARE							
1	Router I						
2	Router II						
3	Switch-24 Port						
4	Server Racks (42U)						
5	Wall Mount Rack (9U)						
6	Firewall and Intrusion Detection & Prevention System						
7	NMS and SLA monitoring software						
8	Patch chord 1 meter						
9	Patch chord 2 meters						
10	UTP cables Box						
11	Patch Panel						
12	Any Other (Please Specify)						
	INR 0.00						

iii) System (Server) Software

S.No.	Particulars	Unit Price in Rs. (P)	Tax(t)	Total amount /unit T= P+t	Total Qty(Q)	Total amount (P+t) *Q	Remarks
1	O/S for Server						
2	RDBMS (SQL Server 2008 Enterprise Ed.)						
3	AV Server						
4	Anti Virus Client						
5	MS Office Suite						
6	Others (Please Specify)						
	Total Cost of equipments for the Server Software						

iv) Power requirements Cost

S.No.	Particulars	Unit Price in Rs. (P)	Tax(t)	Total amount /unit T= P+t	Total Qty(Q)	Total amount (P+t) *Q	Remarks
1	UPS 10 KVA						
2	UPS 5 KVA						
3	Others (Please						

S.No.	Particulars	Unit Price in Rs. (P)	Tax(t)	Total amount /unit T= P+t	Total Qty(Q)	Total amount (P+t) *Q	Remarks
	Specify)						
	Total Cost of equipments for the Power requirements						

v) Manpower Cost

S No.	Resource level	Responsibility& Certifications	Cost/man month	No. of resources	Total Man months	Total Cost
1.			INR 0.00			INR 0.00
2.			INR 0.00			INR 0.00
3.			INR 0.00			INR 0.00

vi) Implementation cost

S.No.	Particulars	Total Units (A)	Unit Value in Rs. (B)	Total Value in Rs (C)= (A) * (B)
Installation				
1				
2				
Commissioning				
1				
2				
Other Cost				

1				
Total				

vii) Other Project Related Cost

S.No.	Other Cost Item	A	B	C
		Cost Per Unit	No of Units	Total Cost of Unit
1.	Cost Item 1			INR
2.	Cost Item 2			
3.	Cost Item 3			
	Total Sum(C)			