



**HLL Lifecare Limited**  
**(A Government of India Enterprise)**  
Corporate and Registered Office,  
HLL Bhavan, Poojappura,  
Thiruvananthapuram– 695 012  
Kerala, India.  
Phone: 0471 – 2354949  
Website: [www.lifecarehll.com](http://www.lifecarehll.com)

### **Invitation for Bids**

#### **Supply of Antivirus Software Licenses for our Offices and Factories**

Date	:	29 <sup>th</sup> June 2013
IFB No.	:	HLL/CHO/IT/Software/2013

**The schedule of the bid is given below.**

<b>Last date and time for receipt of bids</b>	<b>:</b>	<b>15.00 Hrs on 09.07.2013</b>
<b>Time and date of opening of Bids</b>	<b>:</b>	<b>15.30 Hrs on 09.07.2013</b>

Dear Sir,

**Sub: Supply of Antivirus Software Licenses for our Offices and Factories.**

HLL Lifecare Limited Thiruvananthapuram now invites the competitive bids from the eligible bidders to supply of **1500 Nos of Antivirus Software licenses at our Offices and Factories all over India.** The detailed specifications are given as **Annexure-1.**

Sl. No	Item	No of Licenses
1	Antivirus Software Licenses for 1 year	1500

**Terms & Conditions**

1. The respective bidder should have minimum 3 years experience in Antivirus implementation. The following documents are to be attached along with bid;
  - a) Certificate of Incorporation.
  - b) Audited Balance Sheet and Profit & Loss Account or Annual Report for the last three financial years
  - c) Self-certificate stating that the bidder has not been blacklisted/debarred by any institution of the central/state Government/PSU.
  - d) The documentary evidence like work orders, certificate from the clients for the similar works done for the past three years.
2. The prices should be quoted as per the format for price schedule enclosed as **Annexure – 2.**
3. Total Price of the Antivirus Software including licenses and Support Charges for one year should be mentioned clearly in the bid.
4. The bids will be evaluated by taking the total amount for the implementation;  
Total Amount = Cost of 1500 user licenses of Antivirus Software  
+ Support Charges for 1 Year.
5. The supplier has to supply the product with license at Head office and necessary support should be provided for installation.
6. The Authorization Letter from the OEM of the product quoted should be submitted along with the bid.

7. The contact Numbers with single point of communication for technical support across India should be provided along with the bid.
8. The prices quoted shall be valid for a period of 90 days from the date of opening of bids.
9. The items should be delivered within **3 weeks** from the date of placement of order.
10. Penalty at 0.5% per week's delay subject to maximum of 5% is applicable for delayed delivery.
11. Necessary documentations/CDs/DVDs are to be supplied along with the product.
12. Statutory documents like licenses if any should be supplied along with the product.
13. Bids should be clear in all respects and those with ambiguous clauses shall be summarily rejected.
14. The supply order will be placed on the first lowest responsive bidder.
15. The periodic updates from OEM should be available at free of cost during the support period.
16. Necessary support should be provided as and when required within 2 Hrs of intimation of problem.
17. HLL will have the right to increase or decrease up to 20% of the quantity of licenses specified in the schedule of requirements without any change in the unit price or other terms and conditions at the time of placing the order as well as during the support period of one year.
18. Payment will be released within 30 days from the date of delivery and installation of the items.

For claiming this payment the following documents are to be submitted.

- a) Invoice
  - b) Installation report/delivery Chelan signed by both the user and the supplier's representative.
  - c) Statutory documents if any,
19. The bids should be submitted at the following address.

**Associate Vice President (IT)**  
**HLL Lifecare Limited**  
**Corporate and Registered Office,**  
**HLL Bhavan, Poojappura,**  
**Thiruvananthapuram – 695 012,**  
**Phone: 0471- 2354949.**

20. Bids should be submitted on or before **15:00 Hrs on 09.07.2013** and the same **will be opened at 15.30 Hrs on the same day** at Corporate Head Office, Poojappura, and Thiruvananthapuram in the presence of the

representative of the bidder who chooses to attend. If the bid opening day is declared as holiday for HLL, the bid will be opened at the next working day of HLL.

21. The envelopes containing the bid should bear the Invitation for Bids title and number, and the statement DO NOT OPEN BEFORE \_\_\_\_\_ (Here insert time and date of bid opening)
22. HLL reserves the right to accept or reject any or all of the bids without assigning any reason whatsoever
23. Any bid received after the deadline will be rejected
24. No fax/email bids will be accepted

Thanking you,

Yours faithfully,

**P. Sivakumar**  
**SM (Hardware)**

## Specifications

## Annexure-1

<b>Security Protection for Desktop/Laptop Computers and Servers.</b>	<ul style="list-style-type: none"><li>• Solution should provide Security features like Antivirus, Antispyware, desktop firewall, HIPS, Device Control in a single agent which can be deployed ,administered and updated in a single agent package and update mechanism.</li><li>• There should not be any need for multiple deployments of agent and to get the updates to achieve the all product functionality required above.</li><li>• Security and compliance check both should be managed by a single administration management server and console.</li><li>• The agent should be able to password protect uninstall.</li><li>• The agent has the ability to protect the service from being stopped, even if an administrator logs on.</li><li>• Solution should be able to detect and block malicious software in real time, including viruses, worms, Trojan horses, spyware, Adware, and Rootkit.</li><li>• Endpoint Solution technology should include a behavioral based technology apart from providing the signatures for known threats, vulnerability and heuristic based approach.</li><li>• It should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.</li><li>• Solution firewall engine should have option to allow and/or block support of network protocols, including Ethernet, Token Ring, IPX/SPX, AppleTalk, and NetBEUI.</li> <li>• Solution can block protocol drivers (example: VMware, WinPcap) and should have Adapter specific rules like Ethernet , Wireless, VPN</li><li>• Proposed IPS solution should allow customer to edit and create the IPS signature using snort based format if required.</li><li>• Proposed Solution should have the NAC agent installed by default and it can be disabled.</li></ul>
--	--

	<ul style="list-style-type: none"> <li>• Antivirus Solution should provide a tool to scan the offline VMware image for threats</li> <li>• The proposed AV client should have a visible indication whenever it connected to the AV console.</li> </ul>
<p><b>Management Console</b></p>	<ul style="list-style-type: none"> <li>• Solution should provide integration with RSA for management console authentication addition to the user credential authentication, if required and also should get integrated with LDAP, Syslog, and Active Directory.</li> <li>• The Management servers installed at different locations should have the ability to replicate data, logs and content at defined interval in Multi-Server Architecture with Policy and Log Replication.</li> <li>• Management Server should support storing policy and log data in SQL Databases or embedded database.</li> <li>• Management server should support Microsoft Windows 2003,2008,Microsoft Windows XP, Windows 7, Microsoft Windows 2000 (SP3 and later) 32-bit.</li> <li>• Agent should support Microsoft XP/Vista/Windows 7/Windows 8 32 bit &amp; 64 bit and Microsoft Windows 2000/2003/2008 clients.</li> <li>• Anti-virus should also support Red Hat® Enterprise Linux, SuSE Linux Enterprise (server/desktop), Novell® Open Enterprise Server, VMware, Debian etc.</li> <li>• Update - Update mechanism should include client content updates from management server, internal update servers, external vendor update servers, also from the client that acts as a proxy between a management server and clients in the group and using Third-party tools like Microsoft SMS.</li> <li>• Proposed Solution should be able to deploy flexible and different security policies depending upon the AND/OR relationship of following network triggers - <ul style="list-style-type: none"> <li>• IP address (range or mask)</li> <li>• DNS Server</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>● DHCP Server</li> <li>● WINS Server</li> <li>● Gateway Address</li> <li>● MP Token Exists (hardware token)</li> <li>● DNS Name Resolves to IP</li> <li>● Policy Manager Connected</li> <li>● Network Connection (wireless, VPN, Ethernet, dialup)</li> </ul>
<p><b>Firewall and IPS</b></p>	<ul style="list-style-type: none"> <li>• Proposed IPS solution should combine NIPS (network) and HIPS (host) both with Generic Exploit Blocking (GEB) for one signature to proactively protect against all variants, Granular application access control and behavior based technology mentioned above.</li> <li>• System Lock Down - it should be able to “Locks down” the system by fingerprinting every executable file on the system. It can then monitor all running applications and terminate any application for which the agent does not have a matching fingerprint.</li> <li>• Desktop Firewall rules should be configurable depending upon the adapters including Ethernet, wireless, Dialup, VPN (Microsoft PPTP, Nortel, Cisco.</li> <li>• Desktop Firewall rules should be configurable depending upon the state of screen saver "ON" &amp; "OFF".</li> <li>• Desktop Firewall Policies should be configurable depending upon the time and day.</li> <li>• Product should have readymade policies including -To Make all removable drives read only , To block program from running from removable drives , protect clients files and registry keys , log files written to USB drives , block modifications to host files</li> </ul>