

Licensee Hardware Requirements

Terminal Service - Remote Desktop Method*: PC Computer running Windows XP (SP2 with RDP 6.1 OR SP3) OR Windows Vista or Windows 7 running Remote Desktop 6.1 or later with a minimum screen size of 1024 x 768. High-speed connection to the internet (minimum of 512 Kbps download and upload bandwidth). (Testing showed a Peak Bandwidth Download of 50 Kbps). Terminal Server compatible printer.

Data Center Hosted Site Information

LVM uses PC hardware/software that meets or exceeds the following standards:

MS-SQL Server - (or Similar)

Dell Power Edge 1950
Intel Xeon L5410 2x6MB Cache,
2.33GHz, 1333MHz FSB
4GB 667MHz RAM (2x2GB), Dual Ranked DIMMs, Energy Smart, PE
2 - 73GB 15K RPM Serial-Attach SCSI 3Gbps 2.5-in Hot-Plug Hard-Drives

Microsoft Small Business Server 2003 R2 with SP2 Premium Edition
OR Small Business Server 2008 Premium Edition
Elusiva Terminal Server Pro OR Terminal Server Licenses
Appropriate number of User CALs (client access licenses)
Terminal Server/Remote Desktop connections with 128 bit Encryption enforced

*LVM will scale the solutions to the number of concurrent licenses.

Hosting Facility Features:

- 10 Mbps of blended internet bandwidth across multiple tier 1 providers
- Carrier-neutral network access
- 100% Uptime with a Service License Agreement of power and internet
- Anonymous Locked Cabinets with Biometric access control
- 24/7 Hour Support and Security with access control tracking
- Fire detection and suppression
- Power Generation Backup

LVM currently uses i/o Data Centers - <http://www.iodatacenters.com> .

i/o Data Centers Service Level Agreement with LVM Systems can be found on their website.

Data Backup

LVM will make regular daily backups on the given SQL Server on a second physical drive in the server. The SQL Transaction log will also be stored on this second physical drive. On a weekly basis, LVM will

also download to a second physical site, such as the LVM data center, an encrypted backup of the SQL database. LVM will also download to a second physical location, on a daily basis, an encrypted download of the SQL transaction logs. LVM may also choose to use a SQL Transactional Replication method for backups at a second physical location. SQL Backups may affect the response time of the application; therefore LVM will work with the Licensee to select the most appropriate time of day for the backup.

Faxing Option and Phone Charges

The VCC allows for faxing of reports or Triage Encounter Charts. The cost associated for faxing services will be billed back to the Licensee at LVM's cost.

LVM Service Level Agreement

Single Site Service Level: LVM will provide 99% scheduled availability of the **Centaurus application***, excluding your local connection to the internet. For each hour the **Centaurus application*** is not available beyond the 99% scheduled availability level, LVM will extend the use of the software by two hours at the end of the contract for no additional cost. Each VCC client has it owns server(s), they are not shared with other clients. Therefore what reports or users run on your dedicated server(s) can impact your response time and service level.

Second Site Hot Location Service: If Licensee selects the option for a Second Site Hot Location Service, LVM will provide 100% scheduled availability of the **Centaurus application***, excluding your local connection to the internet. For each hour the **Centaurus application*** is not available beyond the 100% schedule availability, LVM will extend the use of the software by two hours at the end of the contract for no additional cost. Licensee may elect to have the Second Site Location in a "Cold State." If so, then the 99% scheduled availability service level applies.

Scheduled Maintenance Time: At some point, maintenance or scheduled downtime will be required. The need for this can be based upon, but not limited to, upgrades to the software application that require an update to the SQL databases, re-indexing of the SQL database, installation of hard disks, replacement of power supplies or forced relocation to a new area of the data center by the hosting site. In all scheduled maintenance time cases, LVM will work with you in good faith to notify and minimize any impact this may have on availability of the application.

***Centaurus application** is defined as the ability to use the Centaurus software to take calls and does not extend to related products of Faxing, HL7 Interface, WebLink push/pull applications which rely on communications or connections to data sources outside the control of LVM. Any extension of the use of the application as the result of downtime carries no cash value and can only be redeemed through extended use of the application.

Hardware Failure: In the event of a hardware failure, LVM shall keep on-hand ready-to-go server(s), in a "Cold State," with the necessary operating and SQL software to make the transition to a new server as quick as possible. This is known as N+1 level of backup.

HIPAA Business Associates Agreement: All Licensee data associated with this agreement shall be deemed confidential and shall be treated as such and each Licensee and LVM will enter into an appropriate HIPAA Business Associates Agreement.

Acceptable Use Policy

This Acceptable Use Policy document (the "Policy"), including the following list of Prohibited Activities, is an integral part of your Agreement with LVM. Please read this Policy carefully. If you engage in any of the activities prohibited by this Policy, LVM may exercise a variety of legal remedies, including the suspension or termination of your network access and/or account with LVM.

This Policy is designed to help protect LVM and the internet community in general from irresponsible and/or illegal activities. The Policy is a non-exclusive list of the actions prohibited by LVM and LVM reserves the right to modify the Policy at any time, effective upon posting on our website. LVM reserves the sole and absolute right to interpret, apply, define and implement this Policy.

Prohibited Uses of LVM Data Centers Systems and Services, include the following:

1. Transmission, distribution or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.
2. Sending Unsolicited Bulk Email ("UBE", "spam"). The sending of any form of Unsolicited Bulk Email through Licensee Data Centers' systems is prohibited. Likewise, the sending of UBE from another service provider advertising a web site, landing page, email address or utilizing any LVM resources, is prohibited. LVM accounts or services may not be used to solicit customers from, or collect replies to, messages sent from another Internet Service Provider where those messages violate this Policy or the policy or terms of service of another provider.
3. Running Unconfirmed Mailing Lists. Subscribing email addresses to any mailing list without the express and verifiable permission of the email address owner is prohibited. All mailing lists run by LVM customers must be Closed-loop ("Confirmed Opt-in"). The subscription confirmation message received from each address owner must be kept on file for the duration of the existence of the mailing list.
4. Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this Policy or the policy of any other Internet Service Provider, which includes, but is not limited to, the facilitation of the means to send Unsolicited Bulk Email, initiation of pinging, flooding, mail-bombing, or denial of service attacks.
5. Operating an account on behalf of, or in connection with, or reselling any service to, persons or firms listed in the Spamhaus Register of Known Spam Operations (ROKSO) database at www.spamhaus.org.
6. Unauthorized attempts by a user to gain access to any account or computer resource not belonging to that user (e.g., "hacking" and/or "cracking").
7. Obtaining or attempting to obtain service by any means or device with intent to avoid or reduce payment.
8. Unauthorized access, alteration, destruction, or any attempt thereof, of any information of any LVM customers or end-users by any means or device.
9. Knowingly engage in any activities designed to harass, harm or cause damage to Licensee or a third-party, including denial-of-service (e.g., synchronized number sequence) attacks directed at any other user, whether on the LVM network or on another provider's network.

Virtual Call Center - Data Center Hosted Appendix – Page 4

10. Using LVM Services to interfere with the use of the LVM's network by other customers or authorized users.

Licensee Responsibility for Licensee's Users

Each Licensee is responsible for the activities of its users and, by accepting service from LVM, is agreeing to ensure that its customers/representatives or end-users abide by this Policy.

If violations of this Licensee Acceptable Use Policy occur, LVM reserves the right to terminate services with or take action to stop the offending customer from violating this Policy as LVM deems appropriate, with or without notice.