



World Class Security

- PCI Level 4 Compliance
PCI DSS Certificate
- All data is backed up daily
to additional storage
devices.
- Staffed 24/7/365 by
advanced technical and
security personnel.
- To ensure continuous
operation, LeadMaster
manages fully redundant
data lines.
- Security patches are
monitored and kept up to
date on all servers.

LeadMaster Security and Infrastructure Advanced Security Systems

Infrastructure

The LeadMaster application resides on state-of-the-art industry standard Microsoft Windows servers in a VMware environment. To maximize uptime, LeadMaster uses Storage Area Networks with RAID Level 50 and hot-swap drives. VMware provides for both high availability and fault tolerance. In the event of system failure, VMware automatically moves applications and data to other systems.

PCI Compliance

The gold standard in security, LeadMaster is certified as Level 4 PCI compliant. The certificate is attached at the end of this document.

Physical security

LeadMaster's production equipment is housed at a **world-class network operations facility**. Staffed 24/7/365 by advanced technical and security personnel, the restricted access data center enforces strict security measures to ensure security of equipment and data, including multiple identification checks. This facility possesses a Class-A government disaster rating against hurricanes, power failures, nuclear fallout and war related threats. The data center is equipped with multiple backup systems in the event of power failure including an uninterruptible power supply (UPS) battery backup power and fully redundant diesel generators.

Reliability

To ensure continuous operation, LeadMaster manages fully redundant data lines from multiple carriers. In the event that one carrier experiences an outage, all system traffic is transferred to an alternate carrier.

Perimeter defense and internal systems security

LeadMaster has taken rigorous measures to ensure the security of its network and servers as well as all data residing on the system. All data travels over a secure network with personnel strictly adhering to all security precautions. Multiple firewalls with automatic fail-over and operating system lock-down methods are in place to prevent unauthorized access. To further our intrusion detection procedures, our staff continually reviews security and network logs to identify vulnerabilities. Security patches are monitored and kept up to date on all servers. For additional protection LeadMaster offers the option of allowing access to data only for specific IP addresses. Unauthorized data access can also happen from inside an organization so sessions without user activity will automatically be timed out at a user specified interval up to 120 minutes.

LeadMaster custom user security permissions are defined in a security matrix developed in consultation with each client.

Clients are in their own encrypted database.

Data backup

Full data backups are performed daily and incremental backups are performed hourly to Network Attached Storage. Backups are stored for 30 days.

Data encryption

All data flowing between LeadMaster and clients is secure / HTTPS. Browser encryption is 128-bit SSL data encryption in order to protect all client data transmitted to and from the system via the Internet. A signed security certificate ensures that confidential information cannot be viewed, intercepted or altered. Users trying to logon via HTTP are automatically switched over to HTTPS.

User authentication

Logon to the LeadMaster system requires verification of a unique username and password. Optional enforcement of secure passwords includes enforcing: a minimum number of characters, upper & lower case, a number in the password, a symbol in the password, limiting the number of retries before lockout, password expiration and limiting the reuse of passwords.

Access control

LeadMaster controls access to each client database as well as to specific functions within the system. Custom user security permissions are defined in a security matrix developed in consultation with each client. This matrix identifies the client's unique user types and defines the access privileges imparted to users in each group. This system allows both flexibility and tight security, as it can allow or prohibit access to any or all functions within the system, as well as limiting access by assignment, geography, zip code, campaigns, lead status, sales stage, opportunity or anything else available in the search engine.

Logging

User activity within the system is logged to provide clients with an audit trail if the need arises.

