



## PREMIERCARE CONNECT SYSTEMS DATA SECURITY

Leading Edge Technology to provide peace of mind

### FEATURES:

### DESCRIPTION:

Data Center Facility	All Connect Program data is maintained at a \$60 million state-of-the-art, purpose built facility - fully equipped with redundant building systems that guard against power outages, fire hazards, and security threats, managed by one of the leading Managed IT companies in North America. The floor in the data center is raised 24-inches to accommodate under-floor cabling, cooling and to provide clear access to all servers. The servers are housed in Telcordia NEBS-3 compliant seismic cabinets attached to the steel structure and floor bracing that support all equipment through zoned-4 seismic activities.
Security	The data center restricts access only to authorized personnel. Access is permitted with three levels of entrance security: Biometric palm scanner, personal identification number (PIN), and security card to ensure controlled access to the equipment. On-site security personnel monitor security from behind NATO small bore missile ballistic glass and perimeter wall vibration sensors, security alarms, and digital surveillance video cameras monitor and record entry and exit to prevent unauthorized entry.
Power Protection	Power protection is provided through five uninterruptible power supplies with battery backup to ensure a clean and stable supply of power. The power is "phase switched" between the UPS to eliminate spikes in the event of a fail-over. Each server is provided with independent, fully redundant power circuits fed by power distribution units. Three power generators with 72 hours of on-site fuel are automatically activated in the event of a power disruption.
Internet Access	Three separate fully redundant tier-1 Internet backbones enter the facility from underground access ports. These connect using BGP-4 as the external routing protocol. The BGP protocol enables fast routing based on the shortest available path. In the event of a failure, traffic is diverted through another backbone. All Backbones are connected to redundant gateway routers and core switches for redundancy.
Environmental and Fire Suppression Controls	Environmental systems include multiple independent Liebert cooling units with redundant chillers. Temperature and humidity are electronically controlled through sensitive moisture sensors located throughout the facility. Fire suppression is provided through an Inergen gas system and a multi-zone, pre-action dry pipe sprinkler system; each sprinkler head has its own zone, monitored by a multi-zone smoke and fire detection system.
Data Protection	Firewall intrusion protection from computer viruses and hackers is provided and supported with real time monitoring 24-7-365 by data center personnel, is provided by fully redundant Cisco Secure PIX firewall infrastructure. Data center personnel ensure that the firewall structure is the latest most up to date to protect against known threats and to anticipate attacks from unknown sources. All Connect data transmitted between the Data Center and a customer's location is encrypted to provide maximum security and protection of sensitive information.
Computer Hardware	Data is hosted using Oracle 10g RAC on a set of active-active load balanced servers. The servers and shared storage are approved and certified on the Oracle platform by a major brand name hardware manufacturer. Multiple web servers are placed behind redundant load balancing equipment to provide redundant web access to the application.
Data Backups	An incremental backed up of data is performed every 12 hours with full backups performed once a week. One copy is stored in a secure off site location and a second working copy kept onsite in the latest robotic SAN (Storage Area Network) for fast recovery of data if it is ever required.
Some thoughts about Data Security	<p>Gartner Group, a leading U.S. based research firm focused on trends in information technology, estimates that two out of every five enterprises that experience a computers disaster will go out of business within five years of the event. Ernst and Young suggest that more than 30% of companies believe that computer system failure is the most significant threat to their business, with nearly 60% believing the risk to be moderate to high."</p> <p>- - <i>"Canadian Underwriter" June 2003.</i> - -</p> <p>"For many small and medium-sized companies, it's impossible to find the resources or the expertise to fend off the rapidly growing number of attacks and keep patching up software vulnerabilities, "We can wear the pager and be there to do the security fixes, while they can focus on running their business."</p> <p>- - <i>"Report on Business Magazine" November, 2003 Data Center CEO</i></p>