CelAccess Systems

Systems and Network Security

The CelAccess system includes security at many levels including device, wireless network and our servers. These combine to make our system extremely secure and highly reliable.

CelAccess devices have custom embedded software that cannot be read or copied by anyone (compiled code). They communicate over the digital data part of the cellular networks via encrypted, private VPN connections. Devices are addressed using internal, private IP addresses on a publicly non-routable network. Our devices are configured at the cellular network level to only communicate with our servers. Our servers are connected to the networks using encrypted, private VPN connections. Additional software in the devices is configured to only send messages to and only receive messages from our server IP address. As a result of these multiple layers of security, it would be impossible for them to send messages to the devices or receive information from the devices.

All databases used in the CelAccess system are behind dual firewalls on internal networks, and are triple-DES encrypted. All access to the application web site requires authentication and use of SSL encrypted connections.

The data centers include the following security features:

- DWDM powered multi-10 Gigabit Ethernet backbone.
- Connected to multiple diverse upstream providers totaling 9 Gbps of Tier-1
- nternet Bandwidth.
- Full BGP peering with all providers.
- Fully redundant (N+1) power and air conditioning system.
- Advanced fire protection, suppression, and detection systems.
- Power and network connectivity have two diverse paths into facility.
- Fully integrated Monitoring System for all critical building, server and network systems.
- State of the art Security Technology and 24x7 on-site security staff.
- Biometric security systems restrict access to data center locations.
- Closed circuit TV monitoring of all data center entrances.