



SECURITY

Our Commitment to Security & Privacy

To conduct successful business over the Internet, organizations must take security very seriously. Given UnBoundSOUND Web-based business model, we want to assure you that the issue of security has been addressed at all levels by the implementation of rigorous standards and industry-leading best practices. Whether you're accessing your account, storing data or exchanging credit card information, you can feel confident that every exchange and transaction you make is secure.

Account Access

Your information is stored in your personal on-line account. Only you have access to your information, via your User ID and Password. Your User ID and Password are both unique to you and you alone. You control when you change your password and you can change it as often as you wish. Once account access information is received by our application system, it is securely stored encrypted.

Your Session

128 bit Secure Sockets Layer (SSL) technology has been implemented to protect key information exchanges within our application system. 128-bit encryption through SSL is the highest level of protection possible for standard web browser transactions. Information exchanges and transactions, including single- sign-on authentication, contact databases (uploading, editing and storing online), credit card transactions, and billing-related data are strictly protected using this technology. This ensures that your sensitive data is completely private and secure from both external systems and other customers using our system.

Your Data

We understand the importance of maintaining total security of your data. Whether it is your contact lists, your campaign results or your billing information, we've taken many measures to keep your information secure from hackers, other customers and other systems. Data files for client contact lists and client data are stored separately to provide privacy and integrity between files. This structure is replicated per customer to extend privacy and security between customers. As well, data files are locked through industry leading Access Control List (ACL) technology — a leading file security practice that ensures only accredited users have access to the files. Our database is secured behind redundant firewalls and the data is intentionally distributed in a manner that makes it extremely difficult to use without first having the database design.

Your Credit Card Information

Credit card information is transferred to a financial clearing-house using industry-leading, secure transmission technology including SSL and HTTPS (Hyper Text Transfer Protocol Secure). The information is then encrypted using Data Encryption Standard 3 (Triple DES) and stored securely so that it is ready to handle your transactions. Financial transactions are verified through VeriSign®, the leading provider of Internet security solutions. Verisign is accredited by all major security, privacy and Certification Authorities (CAs).

Our Production Platforms

Our production platforms are hosted by a leading provider of scalable, secure Web managed application hosting. Our security coverage extends to include:

Hardware and Software Security

Hardened kernel versions of our application platform, database platform and operating system platform provide enhanced protection at all levels against systems intrusion. CERT and manufacturer's advisories are continuously monitored, and Operating system and Application security patches are regularly applied

to all servers. All systems are monitored for hardware, performance, CPU, memory utilization and unusual activity with real-time 24-hour paging to support staff.

Network Layer Security

All application and database servers are secured behind a redundant firewall configuration providing state-of-the-art Application Proxy and Denial Of Service (DOS) attack filtering. All administration of systems is performed through a Virtual Private Network (VPN) using 3DES encryption. Systems such as our database servers are further protected by the fact that they do not have publicly accessible Internet addresses — they can only be accessed via a private Virtual Local Area Network (VLAN) and through the VPN. Strict network monitoring, intrusion detection and response systems are in place to detect unusual traffic activities.

Physical Security

All application servers are located in an unmarked, dedicated data center facility in a private locked cage, with access restricted to authorized personnel only. Access is permitted with different levels of entrance security - personal identification number (PIN), and security card to ensure controlled access to equipment. The security area is protected by 2.5" NATO small-bore missile and bullet resistant glass. On-site security personnel monitor all perimeter doors, security alarms, and digital surveillance video cameras monitor and record entry and exit to prevent unauthorized entry.

Power to the facility is provided from 2 independent substations, and is protected through 3 X 400KVA and 2 X 750kVA uninterruptible power supplies with battery backup to ensure a clean and stable supply of power. The power is "phased-switched" between the UPS to eliminate spikes in the event of a fail-over. Emergency 2 X 1.5MW and 1 X 1.25MW diesel power is automatically activated in the event of a power disruption. Diesel generators have 72-hours of on-site diesel supply.

The facility provides state-of-the art Very Early Smoke Detection Alarm (VESDA®) for multi-zoned pre-action fire detection and dry-pipe suppression systems.

Backup & Recovery

Redundancy is the key to data recovery. Your data is kept safe with real-time transaction logging, disk mirroring, and daily backups to both disk and high-speed tape. The database servers have triply redundant power supplies, and all data disks are Hot Swappable, and configured in striped redundant mirror configurations for the highest performance and recovery capability. If any disk fails, its has an exact duplicate mirror that takes over to transparently handle all transactions until the failed disk is replaced, with no impact to your data. Weekly backups are stored offsite at a certified facility for added security. Our tape retention strategy ensures that backup data is removed from offsite storage every 2 months.

Privacy

Customer privacy is a prime concern at I-Mobile-AdVantage. We access customer accounts only with the customer's permission and only to investigate a potential problem. We never sell, rent, or share you contact lists or our own customer lists and customer data to any outside firms. UnBoundSOUND never uses your contact lists for its internal marketing purposes. In addition, UnBoundSOUND never makes any personal information about its clients available to any individual or company.

The Bottom Line

Safeguarding your personal and business information is of paramount importance to us as it helps foster confidence, goodwill and stronger relationships with you, our customers. If, at any time, you have questions or concerns about our privacy practices, please feel free contact us at contact@unboundtech.com.