

### **User Authentication and Access Control**

Logon to CRMonCall.com hosted systems requires verification of a unique username and password, which the user may send encrypted via SSL. CRMonCall.com 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 bestowed to users in each group. This protocol allows both flexibility as well as security, as it can allow or prohibit access to any or all functions within the system. Strict custom password management schemes may be utilized to specify elements such as minimum length and alphanumeric requirements with account lockout occurring after a set amount of incorrect attempts. Re-activation is then authorized by the assigned helpdesk personnel.

### **Logging**

User activity within the system is logged to provide clients with an audit trail if the need arises. Visual audit trails within the system also record changes in assignment and campaign and also enable activity tracking to keep a history of emails sent, marketing activities assigned and notes recorded. System-based logs are retained for 60 days; visual audit trail elements include timestamp and username information.

### **Datacenter Infrastructure**

CRMonCall.com hosts the Info@Hand application on state-of-the-art industry standard server platforms. To maximize uptime, each server is configured with RAID Level 5 and hot-swap drives. Our primary production servers are backed up with real-time standby servers waiting to assume the identity of a production system in the event of failure. All database servers are duplicated on real-time back-up servers. Spare hardware is retained onsite in case of emergency requirements.

### **Physical Security**

CRMonCall.com'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 identification checks. This facility possesses a Class-A government disaster rating against hurricanes, power failures, nuclear fallout and war related threats. Our data center location is also equipped with multiple backup systems in the event of power failure or natural disasters, including full redundant battery backup power, a diesel backup generator and hurricane disaster rating.

### **Reliability**

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

### **Perimeter Defense and Internal Systems Security**

CRMonCall.com has taken rigorous measures to ensure the security of its network and servers as well as all data residing on our hosted client systems. All data travels over a secure network with personnel strictly adhering to all security precautions, including enforced password management and encryption

for remote access. Multiple firewalls 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.

The technology employed in the CRMonCall.com firewall infrastructure is industry recognized as a leading high security, high availability solution that offers deep packet inspection (intrusion detection) and real-time fail-over. It also supports extensive logging and reactive threat response.

### **Data Backup**

Data backups are performed in real-time to backup servers on standby to assume the identity of a failed system. In addition, all data is backed up daily to additional storage media devices. Media backups are stored for up to 30 days. Data is stored on a Network Attached Storage (NAS) solution that utilizes failover in order to maximize data integrity.

### **Data Encryption**

CRMonCall.com offers the strongest browser encryption available through 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 are alerted to the secure status by a lock displayed in the browser window.

### **Updates and Patching**

All operating systems are maintained at each third-party providers recommended patch levels for security. Any unnecessary users, protocols, and processes are removed or disabled to further enhance security. We proactively update all servers and appliances with the latest service packs, security patches, and firmware.

CRMonCall.com employs a strict process for maintaining all systems up to date with the Info@Hand recommended patch levels for security to protect against vulnerabilities. All critical updates are automatically installed site wide within one day of the update being issued from the third party provider. All non-critical updates are queued for administrative approval before being installed to prevent any disruption.