



Security Question and Answers

Describe how Customer's information is protected from unauthorized access or disclosure during storage, transmission or processing.

When an authorized user connects to the system through the Internet, the connection is secured using 128 bit secured socket layers, which is verified by a GeoTrust Digital certificate.

How is the integrity (accuracy) of Customer's information protected?

The database server, which houses all completed records, is on a separate sub network that is not connected to the Internet and uses addresses that are not Internet routable. This data network connects to the application servers through a dedicated firewall that only allows data requests that originate from a private IP address on the application server. This protects the database server and the data, as it is not even visible or accessible from the Internet. Only the application server, when accessed by an authorized user using compiled components of that server, can make a connection to the data for a specific record request.

How is the availability (accessibility) of Customer's information assured?

Data is accessible on the system for 60 days and is only available to authorized individual users from the requesting customer. After 60 days the data is archived and stored on separate media and is not accessible by a customer user through the Internet. This archived data can only be retrieved by a special request as a historical view of the original request. .

In the event of a system failure or disaster, how is a Customer's information protected?

With a system failure, all access to servers is terminated. Database server sits behind two firewalls and is not accessible from the outside.

In the event a security incident occurs that affects Customer's information, describe MAF's incident response and escalation procedures (including the notification and involvement of Customer).

Determine the type of incident, take measures to prevent further incidents, investigate what was compromised. Contact customer immediately if their data was compromised.

Describe the technical controls used to support this service or application: user access management, separation of duties, network architecture, and system redundancy.

Web Interface user access is maintained by customer maintenance. The Network Administrator controls user access to Customer's data. Web Server is located behind a firewall and proxy server. The server is not directly accessible from the Internet.

What policies and procedures are in place for user identification and authentication (e.g., user ID, password and encryption)?

A system administrator or customer administrator can only issue the login name. Each user login name is unique to the system. A user picks their own password, which is only known to them. Even a system or customer administrator does not have access to individual user passwords. Passwords must meet the requirements for strong typed:

Must be a least 8 characters

Must have at least one Lower Case letter

Must have at least on UPPER CASE letter

Must have at least one number

Must have at least one special or punctuation character

Passwords automatically expire every 90 days. Each user is required to choose a new password that is different from the previous password prior to the password expiration.

Describe MAF's hiring procedures related to security for individuals who may have access to a Customer's information (e.g. background checks, bonding).

Per policy, employees have background checks consisting of Criminal and Credit.

How does MAF protect itself and any Customer's data from viruses or malicious code?

As needed or notified by the hardware or software vendors, we implement upgraded or updated firmware or software for the firewalls, Internet server and operations systems to ensure that the most current and secure versions are always in place. The firewall and server logs are reviewed weekly to identify any current or recent attacks, or potential attacks that were successfully handled by our security measures.

Describe MAF's change control process in relation to product development, test and implementation, and patch update policy.

Any service or application is first tested in an independent test environment. Once approved, application is then moved to production environment with a test code and an isolated test site. Once approved, application is then moved to live environment with several beta customers.

Where is MAF's operations center (main processing for this system) located and what physical security provisions are in place?

The operations center is in Atlanta, Georgia. The servers are located at an Internet Service Provider (ISP) facility that provides 24 hour a day monitoring. This facility utilizes a card access and CCTV monitoring system to control access to their facility. Personnel requiring access to the data center must be on pre-authorization list and surrender their valid driver's license prior to being able to proceed into the raised floor area. The servers are located in locked cabinets that can only be accessed by authorized technology support personnel. Once inside the cabinets, the server console can only be accessed by authorized technical personnel, using Ids that have strong type passwords. ISP personnel do not have access to data.

Describe what auditing and monitoring processes for networks and systems are implemented where a Customer's information may be processed, transmitted or stored (including audited events and logging, log protection and log retention).

All activity, excluding normal web traffic, is logged by the firewalls. These events include unauthorized connection attempts, blocked attempts, attacks (IP spoofing, Ping of Death and SYN flood), system errors, and administrative access.

Describe MAF's process for complying with the Gramm-Leach-Bliley Customer Privacy Act (15 U.S.C. 6801 and 6805).

There is no disclosure of Customer's information to any third parties be it external or internal. Customer's information is only accessible by Customer's designated users.

Please direct questions to MAF Background Screening to the attention of Robert Krone @ 813 273-7810 or via e-mail to: robert.krone@mascreeing.com