Ministry Mobilizer (Version 8.2)

Web Application Security Overview

March 18th, 2015

Overview

Protect My Ministry will maintain the highest level of security and confidentiality of all personal information and will under no circumstances sell or distribute personal information to a third party, except as provided in our Privacy Policy or when required to do so by law.

Security Overview

Protect My Ministry's data is transferred utilizing secure socket layer (SSL) along with User ID and Password protection, giving each user their own unique account name and password. For each order that is placed, we store the IP address which the order originates from. The login activity and IP address is logged with each login attempt.

Sensitive information such as social security numbers and date of births are obscured on all reports that are accessible via the Internet. The network is protected by multilayer IDS, IPS device and firewall systems, the operating systems are updated on a regular basis to ensure the latest security patches are installed. Our servers are password protected and reside in a secure environment protected from unauthorized access, natural disaster, fire or other compromising conditions. Our environment is co-located facilities in different regions of the United States, so in the event of a regional disaster; personal data remains secure.

Physical Infrastructure

- Data Center is SOC II and ISO certified
- Bio Metric with Key Card to access Data Center Servers
- Guards 24×7
- All persons physically accessing servers are escorted by Data Center security
- Data Center Security unlocks server cage before any work on physical servers can begin
- Continuously available power through redundant UPS systems and diesel generators
- Consistent environmental controls through redundant HVAC systems
- Raised floors and early warning fire detection systems
- Closed-circuit television cameras recording all data center activity
- Multiple security checkpoints to gain access to data center

Network Infrastructure

- Tier 1 ISP backbones to various local loops for redundant OC-3s
- Cisco-powered Internet mesh platform
- Local Loop Providers over SONET
- Hubbed DS-3s for PTP and Frame Relay Connections
- Multiple physical and electronic security layers to safeguard against unauthorized access

Disaster Recovery

Protect My Ministry conducts data backups every 30 minutes on a continuous basis. The data is transferred to a separate backup server so the active data and backups are on different servers. In regards to disaster recovery, our servers are located in a state-of-the-art facility with a 24-7 physical presence and automated monitoring to minimize any disaster events.

We also have multiple database and application servers which client systems can be operated from, so in the case of a failure, we are able to bring client systems online from different servers which are already configured and waiting to be utilized.

Data Retention

Pursuant to the FCRA, we must maintain any reports that we generate for a minimum period of five years. Protect My Ministry maintains written or electronic copies of information received in conjunction with services rendered for a period of seven years in a secure facility which is electronically and physically monitored 24/7/365. Information is subsequently destroyed by means of erasing and destroying electronic files, and pulverizing and shredding written or hard copy materials.