800 319 5581
800 319 5582 Fax
www.protectmyministry.com
www.mobilizemyministry.com

Protect My Ministry websites including www.ministryopportunities.org have the following SSL Certificates and protection:
Extended Validation Certificates provide the highest level of online assurance for your customers using a process that's standardized across all certification authorities:

- More extensive than any existing SSL vetting process (undertaken by any certification authority).
- Verification of our organization's identity, the validity of our request and the overall legitimacy of our business.
- Browsers also display both the organization name and issuing certification authority.
- 256-bit encryption technology Deluxe SSL Certificate proves that our Web site is a secure place for customers to conduct business. Our Secure Sockets Layer (SSL) Certificate enables us to protect transactions and other activity on our Web site with 256-bit Secure Sockets Layer (SSL) encryption.

The actual encryption strength on a secure Web site connection enabled by a digital SSL certificate is determined by the level of encryption supported by the site visitor's browser and the server that the Web site resides on. For example, the combination of a Firefox browser and an Apache Web server enables 256-bit AES encryption with our SSL certificates. That means that if your Web site is hosted on a server whose software supports 256-bit encryption — such as Apache —, then site visitors that use a Firefox browser will have their transactions with your site protected by 256-encryption. Thus with the right combination of Web browser and Web server, you can establish a 256-bit encrypted secure connection via an SSL certificate. Encryption strength is measured in key length — number of bits in the key. To decipher an SSL communication, one needs to generate the correct decoding key. Mathematically speaking, 2^n possible values exist for an n-bit key. Thus, 40-bit encryption involves 2^{40} possible values, 128-bit encryption 2^{128} combinations, and 256-bit keys involves a staggering 2^{256} possible combinations, rendering the encrypted data de facto impervious to intrusion. Even with a brute-force attack (the process of systematically trying all possible combinations until the right one is found) cracking a 256-bit encryption is computationally unfeasible.

PMM Privacy Policy

Your privacy is important to us. To better protect your privacy we provide this notice explaining our online information practices and the way your information is collected and used. To make this notice easy to find, we make it available on our logon page.

Application of This Notice

This Notice applies only to the information collected by PMM from the users of the PMM systems. It does not apply to information collected by PMM in any other way, including offline.

The Information We Collect

Our web sites are not set up to automatically collect personally identifiable information from each visitor to our web sites. It does recognize the home server of visitors, but not e-mail addresses. For example, we can tell which Internet Service Provider our visitors use, but not the names, addresses or other information about our visitors that would allow us to identify the particular visitors to our web sites. This information is used only for internal purposes by our technical support staff.

Our web sites do track certain information about the visits to our web site. For example, we compile statistics that show the numbers and frequency of visitors to our web sites and their individual pages. These aggregated statistics are used internally to improve our web sites and for product development and marketing purposes generally. Those aggregated statistics may also be provided to advertisers and other third parties, but again, the statistics contain no personal information and cannot be used to gather such information.

In a few areas on our web sites, we ask you to provide information that will enable us to verify whether you are entitled to access and use certain information, materials and services available from our web sites, or to enable us to enhance your site visit, to assist you with customer service or technical support issues, or to follow up with you after your visit, or to otherwise support your customer relationship with PMM and it's partners, clients and subsidiaries. It is completely optional for you to participate. However, failure to participate may mean that you cannot access and use certain information, materials and services.
For example, we request information from you when you:
1. Log-on to certain areas of our web sites, where you may be prompted to provide us with your user name and password as a condition to gaining access to certain information, materials or services.
2. Register or sign-up to use a service.
3. Place an order.
4. Provide feedback in an online survey.
In each of the instances above, we typically ask for your name, e-mail address, company address and phone number, product preference information, user name and password, as

well as other similar personal information that is needed to register or subscribe you to services or offers. On occasion, we may ask for additional information to enable us to provide you with access to and use of certain information, materials and services. In the case of newsletters or mailing lists, you will be able to "unsubscribe" to these mailings at any time.

Our Commitment to Data Security

To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect online.

Links to Third Party Sites

Our web sites may include links to third party sites which open in a new browser window after the user is alerted that they are leaving the our web site. PMM accepts no responsibility for the content of these third party sites.

Cookies and Logs

Cookies are used only by our systems to allow users to visit pages without logging on more than once. Cookies are never stored or used to gather any information other than to track the activities of a logged on user of our systems where necessary. Cookies do not persist after termination of a user's session. No third party cookies are permitted on our web sites.

Our Background Check Service and servers are located within the Peak 10 Data Center facility and are monitored/ managed by our personnel locally and remotely.

- Your online ordering system and data is housed on our servers in a 25,000 sq ft concrete Data Center which has Level 5 physical Security and cyber security
- You never have to worry about our systems going down
- Backups are performed for data and programs twice, daily
- All updates or fixes are handled proactively by detecting and examining error logs
- Our facility has redundant power, UPS and Generators
- Our facility has 3 ISPs, Time Warner, XO Communications (SBC) and ATT (for redundancy)
- Our Firewall, Fort iGATE, is a redundant and PCI Compliant Unit
- Our facility is manned 24/7/365
- We have a real-time performance and reliability monitoring for your site once you come on board

Our Data Center Infrastructure

Facility Facts -

Security
Each Peak 10 facility is engineered with a minimum of five levels of security:

- Level 1: Proximity card access with PIN is required to enter the building. You are not yet in the data center.
- Level 2: Proximity card access with Biometric (fingerprint) scan is required to enter the data center.
- Level 3: All hardware is secured in a locked cage or steel mesh cabinets fitted with combination locks.
- Level 4: Video surveillance cameras are placed throughout the facility and monitored by on-site staff 24x7x365.
- Level 5: Strategically placed vibration detection devices alert Peak 10 personnel of any motion.

Uninterruptible Power
Each Peak 10 data center is engineered with an uninterruptible power system and backup generator to deliver seamless power. In the event of a commercial power failure, our isolated UPS system will provide immediate backup power until our diesel generators take over the load and continue operation of the center.

Redundant HVAC

Peak 10 utilizes best-in-class environmental units to control and monitor the temperature and humidity in each data center facility. Our redundant HVAC system keeps the average temperature in each data center at 70 degrees Fahrenheit to ensure a consistent operating atmosphere for your mission critical technology infrastructure.

Fire Suppression

Peak 10 data centers utilize dry-fire suppression systems that can be deployed manually, or by a sequence of three failures anywhere in a data center zone. Each Peak 10 facility is also fully equipped with smoke and heat detection sensors as well as fire doors and handheld gas-based fire extinguishers.

Other Facility Facts

- Custom-sized Private Cages, Single or Half Cabinets
- AC Power (20-100A 110-208V, Multi-Phase, Custom)
- 24x7 Customer Access with 24 hour staff and security
- Customer Work Stations with Phone and Internet Access

Data Center Physical Location is Charlotte