Website Privacy Policy

Protect My Ministry recognizes its need to maintain the confidentiality of Personal Identity Information (PII). The PII covered by this policy may come from various sources including, but not limited to, employees, clients, applicants, vendors and any PII maintained in its systems.

The scope of this policy is intended to be comprehensive, without disclosing technical details that could be used by those with malicious intent and includes requirements for the security and protection of PII information accessed by Protect My Ministry and its vendors.

Departments named in this policy have responsibility for implementing procedural guidance to ensure that their departmental responsibilities under this policy are communicated and enforced.

Personally identifiable information is information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. including, but not limited to;

- Social Security Numbers.
- Taxpayer Identification Numbers.
- Employer Identification Numbers.
- Drivers license numbers.
- Date(s) of birth.

Vendors: Individual(s) or companies that have been approved by Protect My Ministry as a recipient of PII, from which Protect My Ministry has received certification of their data protection practices in conformance with the requirements of this policy. No PII information can be transmitted to any vendor in any method unless the vendor has been pre-certified for the receipt of such information.

PII Retention: Protect My Ministry understands the importance of minimizing the amount of PII data it maintains and will retain such PII only as long as necessary. A joint task force comprising members of the Accounting, IT, Compliance, Operations and Human Resources departments maintain organizational record retention procedures, which dictate the length of data retention and data destruction methods for both hard copy and electronic records.

PII Training: All new employees who may have access to PII are provided with introductory training regarding the provisions of this policy, a copy of this policy and implementing procedures for the department to which they are assigned. Employees in positions with regular ongoing access to PII or those transferred into such positions are provided with training reinforcing this policy for the maintenance of PII and shall receive annual training regarding the security and protection of PII and company proprietary data.

PII Audit(s): Protect My Ministry conducts audits of PII information maintained by the company in conjunction with fiscal year closing activities to ensure that this policy remains strictly enforced and to ascertain the necessity for the continued retention of PII information.

Where the need no longer exists, PII information will be destroyed in accordance with regulations for destruction of such records and logs maintained for the dates of destruction. Accounting, IT, Compliance, Operations and Human Resources departments under direct supervision of executive management conduct these audits.

Data Breaches/Notification: Databases or data sets that include PII may be breached through authorized or unauthorized access. Upon becoming aware of a data breach, the Compliance department will notify all affected individuals whose PII data may have been compromised, and the notice will be accompanied by a description of action being taken to reconcile any damage as a result of the breach.

The Compliance department will handle breach notifications(s) to all governmental agencies to who such notice must be provided in accordance with requirements specified under these laws. Notices to affected individuals will be communicated by Operations after consultation with the Compliance department as specified under the appropriate law(s). Gramm-Leach-Bliley Act, The Privacy Act of 1974, Fair Credit Reporting Act

Data Access: Protect My Ministry maintains multiple IT systems where PII data may reside; thus, user access to such IT systems is the responsibility of the IT department. The IT department has created internal controls for such systems to establish legitimate access for users of data, and access shall be limited to those approved by IT. Any change in vendor status or the termination of an employee or independent contractor with access will immediately result in the termination of the user's access to all systems with access to PII.

Data Transmission and Transportation

1. Company Premises Access to PII: The Accounting, Human Resources and IT departments have defined responsibilities for on-site access of data that may include access to PII; IT has the responsibility to verify data access requirements for all electronic records. Operations, Accounting and Human Resources have the operational responsibility for designating initial access and termination of access for individual users within their departments and providing timely notice of all changes to IT.

2. Vendors: Protect My Ministry may share data with vendors who have a business need to access PII. Where such inter-company sharing of data is required, the IT department is responsible for creating and maintaining data encryption and protection standards to safeguard all PII that resides in the databases with vendor access. Operations have responsibility to notify IT of any changes to vendor status with the company.

Protect My Ministry does not permit employees or vendors to send or store consumer information or PII outside of the United States or its territories to any third parties. California Code 1786.16.(a)(2)(B)(vi).

3. Approved Storage Devices: Protect My Ministry reserves the right to restrict access to PII in the workplace. In the course of doing business, PII may only be downloaded to approved external storage devices to facilitate company business. To protect PII, the company will requires that any such devices are pre-approved by the IT department to ensure compliance with this policy. Only devices with approved encryption and security protection software will be permitted. The IT department is responsible for

maintaining data encryption and data protection standards to safeguard PII that resides on these devices.

4. Off-Site Access to PII: Protect My Ministry understands that employees may need to access PII while off site or on business travel, and access to such data shall not be prohibited, subject to the provision that the data to be accessed is minimized to the degree possible to meet business needs and that such data shall reside only on assigned laptops/approved storage devices that have been secured in advance by the IT department.

Regulatory Requirements

It is the policy of the company to comply with any international, federal or state statute and reporting regulations. Protect My Ministry has delegated the responsibility for maintaining PII security provisions to the departments noted in this policy. Protect My Ministry's Compliance department shall be the sole entity named to oversee all regulatory reporting compliance issues. If any provision of this policy conflicts with a statutory requirement of international, federal or state law governing PII, the policy provision(s) that conflict shall be superseded. Gramm-Leach-Bliley Act, The Privacy Act of 1974, Fair Credit Reporting Act

Employee Hotline: If an employee has reason to believe that PII data covered by this policy has been breached or that company representative(s) are not adhering to the provisions of this policy, the employee should call or contact a Human Resources representative at the employee's location.

Confidentiality: All company employees must maintain the confidentiality of PII as well as proprietary company information to which they may have access and understand that such information is to be restricted to only those with a business need to know. Employees with ongoing access to such information will sign acknowledgement reminders annually attesting to their understanding of this requirement.

Violations of PII Policies and Procedures: Protect My Ministry views the protection of PII data to be of the utmost importance. Infractions of this policy or its procedures will result in disciplinary actions under the company's discipline policy and may include suspension or termination in the case of severe or repeat violations. PII violations and disciplinary actions are incorporated in the company's PII new hire and refresher training to reinforce the company's continuing commitment to ensuring that this data is protected by the highest standards.