1. Web Server: Our website is hosted through Google App Engine (Cloud Hosting powered by Google). Google in itself has stringent privacy policy and is pioneer in data security. For more information please visit: https://cloud.google.com/security/

2. Secure Connection: The communications between user's browser and the website as well as the data downloaded are encrypted through SSL certificate (HTTPS) to ensure absolute data security.

3. User Authentication: User login to the server is secured with Digest access authentication system, one of the most secure methods of confirming user identity. However, we are using the password shared over email and have not changed it. We recommend changing the password periodically.

4. Employee Requirements: After login to server, the employees can view the data, import in CSV format and have access of it. The imported data in the system is then used for analysis and sent to the concerned client.

5. Dropbox: Secure Data Sharing: We use "Dropbox" and "Box" for data sharing. The data can be viewed, downloaded and shared amongst those added to that shared folder or has the secret link to the folder.

6. Terminated Employees: We always ensure that terminated employees no longer have access to systems/server that permit access to Confidential or Internal Use Only information.

7. Confidential Data: We ensure that Confidential or Internal Use Only information is not distributed or accessible to unauthorized persons. Workers never share their authorization passwords under any circumstances. Users must avail themselves of any security measures, such as encryption technology, security updates or patches, provided by Data Security Officers. Workers always log off from all applications, computers and networks, when not in use. Along with it; personally identifiable information of respondents removed from the user data and an identification number assigned to each respondent. The correspondence between identification numbers and personally identifiable information stored in a password protected file, transferred (if needed) only through secure file transfer procedures (encrypted data). Upon completion of the study, the file containing names, telephone numbers and any other personally identifiable information deleted, along with the correspondence of names with ID numbers.

8. Trained: We always train our workers so all staff gets training and support necessary to protect data.

9. Data Security Officer: A Data Security Officer works with Information Technology, to support the implementation and monitoring of security.

10. Data Security Accountability– Our IT staff, workforce and management are aware of their responsibilities and what is expected of them. The various types of data is classified so that both workers and management understand the differences. By categorizing data, employees are aware of how to handle each type and which types they are allowed to distribute.

11. Scanning for Vulnerabilities– It is important to find any vulnerabilities in our infrastructure before hackers do. Since hackers will scan for vulnerabilities the minute they are discovered, a We have a routine in place for checking its own networks regularly.

12. Account Monitoring and Control – We always keep track of who is accessing what.