



SECURITY PRACTICES

Physical Access

The Dirigo servers used to provide the Services are located in a controlled access data center leased by Dirigo Design & Development, Inc. Access to the data center is restricted to Dirigo employees or its agents who need access for the purpose of providing the services. Each rack in the data center is locked with a unique three digit combination. Servers are further secured by locked front server bezel. The data center is monitored 24/7/365 by video surveillance. Entrance to the data center is authorized by individual elevator codes and access cards assigned to only the most senior Dirigo associates.

Firewall Access

All Dirigo servers are secured by hardware firewalls. At the time of provisioning no outside ports are open. There are security risks associated with modifying a firewall configuration, particularly opening non-recommended ports. We recommend only opening ports 80 (Hypertext Transfer Protocol), 443 (HTTP Secure), 25 (TCP) and 110 (Post Office Protocol-POP). Any transmission of files to and from the server should be performed while logged into the VPN and under port 22 (SSH- Secure Shell). Opening up database or administration ports globally or even for single IP addresses or a range of IP addresses is not recommended and may result in a failure to meet Payment Card Industry (PCI) requirements.

Dirigo Personnel

- Screening. Dirigo performs pre-employment background screening of its employees who have access to customers' accounts.
- Access. Dirigo restricts the use of administrative access codes for customer accounts to its employees and other agents who need the access codes for the purpose of providing the services. Dirigo personnel who use access codes shall be required to log on using an assigned user name and password.

Reports of and Response to Security Breach.

Dirigo will immediately report (within 24 hours of knowledge of a breach) to you any unauthorized access or release of your information of which we become aware. Upon request, we will promptly provide to you all information and documentation that we have available to us in connection with any such event.

September 5, 2009 revision