

Plaxo Information Security

Plaxo is committed to handling customer information with the highest standards. We maintain physical, electronic, and procedural safeguards that meet or exceed internationally respected security standards, applicable laws and regulations, and industry based best practices. To protect information in our environment, we implement the following industry-proven standards and technologies:

- We protect our systems and networks from the internet with firewall systems. The Plaxo network can only be accessed through ports 80 (HTTP), 443 (Secure HTTP) and 25 (SMTP). All other network ports are filtered.
- We employ an Intrusion Detection System (IDS) to constantly monitor all activity in the Plaxo network. IDS collects network traffic information and analyzed by Symantec, enabling real-time detection of known exploits, denial-of-service attacks, portscans, etc. We are immediately notified if any suspicious activity takes place.
- We employ a Mandatory Access Control system to manage access to resources on all servers, beyond the traditional user/group based access control that operating systems offer.
- We use SSL to encrypt our proprietary protocol for all client/server communications.
- We install a custom "hardened Linux kernel" that has been reduced to the minimum subset necessary to run our service, effectively removing many exploits and potential compromises.
- We use a single point of access to the secure server network which employs certificate-based authentication via Secure Shell (SSH) limited to a select group of employees. The server machines are on their own private network, isolated from outside connections, with the exception of an "administration" host, which requires certificate-based authentication.
- We employ a monitoring system that continually tests all aspects of the service network. We have an abundance of custom-built and commercial monitoring used to safeguard against suspicious activity (especially things that are not necessarily hacks in nature, but potentially abusive incidents while using the system in a normal fashion).
- We host our service at Equinix, considered in the industry as a provider of world-class physical security. All access points are controlled by biometric hand geometry readers, providing financial grade protection of Plaxo's physical network. Other security features include CCTV camera coverage of the entire center, individually locked cabinets within locked cages, manned on-site security on a 24x365 basis, bullet-proof resistant and windowless exterior walls.
- We validate all e-mail addresses of customers who join the Service.
- We encrypt all passwords stored within our database.
- We do not send passwords or request for passwords through e-mail.
- We expire all web sessions.
- We maintain and selectively review activity logs to prevent unauthorized activities from occurring within our computer environment.
- We control access to customer information inside our company by limiting employee access to systems and data based on business requirements.
- We test our security systems regularly, and periodically contract with outside companies to audit our security systems and processes.

The security of Plaxo accounts also rely on customers protecting their Plaxo password. Plaxo strongly urges that customers never share their Plaxo password with anyone. Plaxo representatives will never ask customers for their password, so any e-mail or other communication requesting for a password should be treated as unauthorized and suspicious. If a customer shares their Plaxo password with a third party for any reason, the third party will have access to that account and personal information, and the customer may be responsible for actions taken using their password. Customers who suspect that someone may have obtained access to their password, please change it immediately by logging in to their account at <http://www.plaxo.com> and changing their Profile settings, and also contact Plaxo immediately as described below.

Contact Information

If you have questions regarding this security and privacy statement, please contact us at:

Plaxo, Inc.
1975 Landings Drive
Mountain View, California 94043
support@plaxo.com