SECURITY

Security is a top priority of Eleo. We regularly review our security features and the latest industry standard security tools and products. Eleo is hosted on Microsoft Azure, a leading provider of infrastructure as a service on the cloud. All computer servers, client data and Eleo systems reside and operate within Azure's secure environment. Below is a summary of Eleo's security features –

NETWORK SECURITY

To ensure the security of your data, Eleo contracts all hosting and data storage with Microsoft's cloud product, Azure.

A partial list of the security features provided by Azure include:

- 24 hour monitored physical security: Our servers are physically constructed in Azure data centers. They are managed and monitored to shelter data and services from unauthorized access, as well as environmental threats.

- Antivirus/Antimalware protection: Microsoft's Antimalware is built into our servers to help identify and remove viruses, spyware and other malicious software.

- Automatic Data and System Backups: Full, daily backups of all data and systems stored off-site, in geographically dispersed locations.

- Redundant Utilities: Backup power and connectivity to the internet.

- Intrusion Detection and DDoS: Azure provides intrusion detection and prevention systems, 'denial of service' attack prevention, penetration testing and forensic tools to help identify and mitigate threats.

DATABASE SECURITY

Eleo also provides security features to protect access to your system and data with:

- Authentication: User name and password protection, invalid attempts tracking and logging, failed attempts lockout, password encryption, and email notification of password changes.

- Activity Tracking: Provides activity logs of users – shows time of login and logout, IP addresses, and other tracking information

- Unauthorized Data Interceptions: 128-bit Secure Sockets Layer (SSL) encryption, an industry standard level of security and privacy. The SSL protocol protects HTTP transmissions over the internet by adding a layer of encryption. This ensures that your transactions are not subject to "sniffing" by a third party.