Online donor management software

Make a bigger difference™

ELEO Security Features:

ELEO provides network, facility backup and disaster recovery options that ensure maximum availability and high integrity of your application data through Microsoft's Azure data centers.

24 hour monitored physical security. Our Datacenter is physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.

Monitoring and logging. Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts.

Antivirus/Antimalware protection. Microsoft Antimalware is built-in to our servers to help identify and remove viruses, spyware and other malicious software and provide real time protection.

Intrusion detection and DDoS. Our datacenter provides intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats.

Automatic Backups. ELEO creates daily full disk backups of all data. Full database backups are stored off-site in geographically dispersed locations as an added means of recovery should it be needed.

Unauthorized Data Interceptions. All ELEO communication is secured with 128-bit Secure Sockets Layer (SSL) encryption, an industry-standard level of security and privacy for those wishing to conduct secure transactions over the internet. The SSL protocol protects HTTP transmissions over the internet by adding a layer of encryption, ensuring that your transactions are not subject to "sniffing" by a third party. Only your users, with the right combination of a ELEO Login and Password, can access your data.

SSL is used in tandem with a digital certificate. This digital certificate gives you the assurance that you are connecting only to a legitimate ELEO server, and not that of an impostor. The certificate contains information about who owns and authorized the certificate (company name, domain name, contact address, etc.), encryption levels used, as well as information about the issuing Certificate Authority.

Unauthorized Access - Authentication via username and password provides assurance that a client requesting information is the entity it claims to be. ELEO also provides additional layers of password

security protection within its environment. To prevent brute-force password hacking, invalid login attempts are tracked and logged within the system and accounts are locked out after a number of failed attempts. Critical user information, such as a user's password, is encrypted within our databases. Password resets are performed through an industry-standard self-service process - so even our support staff has no knowledge of your passwords. Email notifications are sent to account holders any time a password is changed.

Database activity logs record information about the username, time of login and logout, the user's IP address, and other information about each ELEO session. This data can be used for auditing purposes and to provide admissible evidence in court proceedings.