Lamplight

Leaving you time for what really matters

Security

Physical security – where are your servers and are they secure?

Our servers are located at the BlueSquare data centre, located near London (see http://www.bluesquaredata.com). The data centre is located within secure compounds with 3-metre fencing and electric entry, including anti-tailgating systems. Entry to the buildings is via a swipe card system, with 6-layer security and 24/7 on-site security. We do not need or have physical access to the servers, and BlueSquare control access to authorised personnel.

Server security – are the servers secure?

Yes. All services that are not needed on the server are turned off. Remote access uses encrypted connections, using non-standard logins and public/private key authentication (and encrypted private keys). Our server provider does not have access to the server or the data on it. All access, and attempted access is logged and logs are checked.

What about the data protection act?

You will probably need to register with the Information Commissioner, if you haven't already (*http://www.ico.gov.uk*). We are voluntarily registered (number Z255706).

Impress your funders, improve your efficiency and demonstrate your impact

Lamplight is a powerful web-based management system for charities. It is flexible, easy to use, and secure, with packages to suit any budget.

Have your data, your way. Switch on Lamplight.

Call us to arrange your demonstration on 020 7558 8793.

Lamplight Database Systems Limited, 19 Eastbourne Terrace, Paddington, London W2 6LG

T: 020 7558 8793 E: enquiries@lamplightdb.co.uk W: www.lamplightdb.co.uk

Company registered in England & Wales no. 5184376. Registered address: 14 Oxford Road, London NW6 5SL

'Filtering and validating data' means that whatever you enter into Lamplight is checked to ensure it's the right kind of data.

'Escaping' data means displaying it on screen safely. It can also refer to a technique for inserting data into the database safely. Lamplight does both.

CSRF (cross-site request forgery) is a hacking technique.

SSL (secure socket level) is a way to encrypt data between a web server and your computer. 256-bit is the 'amount' of encryption.

Application security – is the Lamplight software secure?

Yes. Authorisation and access control across the entire application defaults to 'no access' unless you are logged in and have the appropriate permissions. No application code is located in public directories on the server. Passwords are stored securely (not in plain text), but password policy (strength, frequency of changes etc) are for the customer to decide and adopt.

All data coming into the application are validated and filtered; all data out are escaped, and all forms are 'salted' prevent CSRF attacks. Each customer's data are stored in a separate database, with separate access for each customer. Data changes are logged by who made the change and the date and time of the change.

All data transferred between our server and your computer is encrypted using 256-bit SSL, verified by DigiSign.

Backup security – are the backups secure?

Yes. Daily backups are taken and stored online, and are as secure as the server. Weekly backups are transferred off-site using a secure SSL connection; are then encrypted using 256-bit encryption and stored on a removable hard disk. File deletion uses 3-pass overwriting to ensure data are removed.