Lease-Desk Access and Security F.A.Q.'s:

What is SSL?

SSL encrypts information sent between your website and a visitor's web browser so that it cannot be read as it is sent across the internet.

SSL stands for secure sockets layer, and it's most commonly used when websites request sensitive information from a visitor, like a password or credit card number.

If you've ever bought anything online, you've probably used SSL without realising it. Most web browsers display a padlock when you're viewing a site over SSL, so you know the connection is secure.

The address of pages viewed over SSL also normally starts https://, instead of http://.

What is an SQL Injection?

This happens due to unfiltered requests from a user reaching the database, and being able to alter or manipulate the meaning of queries which are run by the database.

Lease-Desk.com's written code is first careful to filter all user input and uses a technique known as "prepared statements" to protect against this. This enables the database to know the difference between the query code and any user input which may be embedded within it.

What is Cross-Site Scripting (XSS)?

Cookies are normally small packets of identifying data which are sent to the web server by the client on every request. Because a cookie identifies a user, if another user is able to steal another's cookie - they [the attacker] will be able to impersonate the victim.

XSS is where unfiltered input is being displayed back to an end user. This can result in either defacement of a website, or Cookie loss, for any user which views the compromised page.

Lease-Desk.com's written code base removes nearly all HTML tags on input submission, and also escapes all data when outputting it, resulting in increased application security from such vulnerabilities.

What is (Remote) File Inclusion?

This happens when a user can upload code to the server, or make your application load code from another location.
Although Lease-Desk.com does allow end users to upload files to it, when doing so, the files are stored outside of the publically accessible area of the website, with a random file name, which provides two levels of increased protection.

What is E-mail / HTTP injection?

Email injection occurs when unchecked content is injected into the headers of an email (e.g. changing the to/from/subject or adding attachments to the body), which will lead to spam. The site uses the Zend_Mail library to send mail, which is immune from Email injection.

Http Injection occurs where someone can inject data into a HTTP response which will then be returned to the end user. Lease-Desk.com is protected in two ways;

a) PHP includes protection against this in suitably new releases.

b) Our development has meant that Lease-Desk.com only redirects to hard coded addresses (and aren't using user supplied data to perform the redirect).

How does Lease-Desk's Server work?

The server runs Linux which has a proven track record of being more secure than e.g. Microsoft Windows. To be specific, the server runs Debian Linux which has a long history being stable and secure. The current install will be supported for approximately 2-3 years from now - at which point we will upgrade the server to the next version. See e.g. http://debian.org

Our dedicated server will automatically install the majority of updates, and any additional manual installations will be carried out by our software developers periodically.

How does the Firewall work?

The firewall filters Internet traffic to and from the server. Lease-Desk's server has a firewall installed on it which will :

a) Stop the web server from making outbound requests (which is often the route an attacker will make to download malicious code onto a server).
b) The firewall blocks incoming traffic which isn't going to both Lease-Desk.com and a few system services, (ntp (time), DNS, ping and SSH).