Echidna Server Security

Background

Echidna is hosted on a Virtual Private Server (VPS) with Google Cloud Platform (GCP) in one of Google's Sydney zones. GCP meets rigorous privacy and compliance standards that test for data safety, privacy and security. For more information refer to Google Cloud Platform Security and Compliance

Echidna hosting on GCP is managed by AusTiger Hosting who monitor the server performance and respond to any issues. For more information refer to http://www.austiger.com.au

Security

Google Cloud Platform services always encrypt customer content that is stored at rest, with a few minor exceptions. Encryption is automatic, and no customer action is required. One or more encryption mechanisms are used. For example, any new data stored in persistent disks is encrypted under the 256-bit Advanced Encryption Standard (AES-256), and each encryption key is itself encrypted with a regularly rotated set of master keys. The same encryption and key management policies, cryptographic libraries, and root of trust used for your data in Google Cloud Platform are used by many of Google's production services, including Gmail and Google's own corporate data.

In addition to GCP encryption all Traffic between the web servers and end users is encrypted via TLS1.2 and password fields are encrypted within the database as an extra layer of security.

Server Access and Confidentiality

AusTiger manages the server security. The principal of least access is employed as part of Identity and Access Management (IAM) server configurations. Multi Factor Authentication (MFA) is used and SSH keys are securely stored.

Inet Solutions and its personnel access the Customer's data only for the purpose of assisting the Customer in providing Help Desk support.

Redundancy

Google Cloud Platform has extensive redundancy in place as would be expected by this level of service. Google does not disclose their cloud architecture outside of saying "everything is redundant". In the event of a physical host failing the VPS will be immediately restarted on another host. When host hardware maintenance is performed VPS's are live migrated to other hosts within the Sydney region.

GCP and AusTiger each have several layers of automated monitoring and alarms. In the event that services should need restarting, in some cases this is automatic and in others a manual restart will be required.

Backup

Nightly backups are taken on the Server and kept for 60 days. Multiple copies of each backup are stored by AusTiger across various locations. Backups are fully encrypted while in rest and in transit.

An additional backup copy of the data is taken by Inet Solutions on a weekly basis and stored in Newcastle NSW. One backup per month is retained for 6 months.

Pdf Attachments added to clients files are stored through Amazon S3 in Sydney, with additional backups of these kept by Inet Solutions in Newcastle.

In the event of data corruption or deletion the last healthy backup would be restored in a separate location and any corrupted or missing files would be individually replaced. Any restoration of inadvertent data deletion may result in additional charges being levied to cover the associated time.

Auditing

Time Stamps - Screens are stamped with the last updated date and time and login of the User who made the change.

Note Audit Logs – Each note stores a log of updates for key fields.

Sent Email Log – This is a log of all emails which have been sent through Echidna for the past 60 days. This is available as a report which can be downloaded at any time.

SMS Sent – there is a daily emailed report of SMS's sent as part of the overnight run. Additionally reports are available by logging in to the SMS provider's website.

Deleted Appointments - a report is available from the reporting menu which lists any notes deleted by someone other than the consultant who the appointment was for. Additionally deleted appointments are displayed on the notifications screen of the consultant who had the appointment.

Deleted Client Documents - copies of client documents are incorporated into Echidna's long term backup functionality by the overnight backup processing. If the document is accidentally deleted from the client record, a copy can be retrieved by Inet Solutions on request.

Customer Access

The Customer is responsible for maintaining their own usernames and passwords.
Multi Factor Authentication (MFA) is available and is managed by the customer's Administrators.