Echidna Resilience and Cyber Security

Document Purpose

Inetsolutions, the developers and providers of the Echidna Online Database, recognise the criticality of protecting the database content from unauthorised access. This document provides an overview of the security measures that are in place to guard data content and ensure appropriate uninterrupted access.

Application Hosting

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

Austiger apply up to date security patches to the Operating System, and other system software. Automated monitoring software detects and alerts to any potentially suspicious access.

As the application provider, Inet Solutions is vigilant to potential emerging risks, with security being a high consideration in product development.

Server 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 Hardware 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.

A recent option that can be requested is for a weekly backup to be made available and stored on the customer site. This can be used for disaster recovery in the unlikely event that Inetsolutions ceases trading.

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.

All data sent to and from the application is encrypted via TLS.

Operating System access is limited to specific fixed IP addresses maintained by Inet Solutions.

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

confidentiality agreements.

Each customer is responsible for maintaining user access to their instance of Echidna. Password settings are customisable including two factor authentication. Password policies can be customised, including reset period, minimum length, and required mix of characters. In addition, customisable security options are provided which enable access to different options in the software, including client information. All password stored within Echidna are encrypted at a database level.

Further, Inetsolutions are in the process of enabling customers to integrate Echidna into their Single Sign On access to give customers a single point of access control across their suite of applications.

Application Design Security Considerations

The application design includes multiple layers of security safeguards. These include code to guard against sql injection attacks, cross site scripting attacks, man-in-the-middle attacks, and brute-force password attacks.

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.

Key Personnel Continuity Plan

Inet Solutions is reliant on a small number of key personnel to provide software development. It is primarily the skills of the Senior Developer that have made Echidna such a highly effective product.

In the unlikely event that the Senior Developer is unable to work for an extended period, a business caretaker agreement is in place. A skilled software developer with experience working as a consultant on the Echidna project will commence supporting Echidna full time. This will either be a long term replacement or will at least be an interim measure until an appropriate long term replacement is found and trained.

It is important to note that Echidna would continue to function in its current form without any intervention. However, in order to continue development and respond to changing needs an experienced software developer will step in immediately.

The existing customer support, training & help desk team will also be available for customer support.

Ongoing Reviews

This Cyber Security provisions are subject to ongoing review.
If new vulnerabilities are identified or additional safeguards become available these will be added to the plan as appropriate.