INSTITUTE OF POSITIVE EDUCATION

IT SECURITY SUMMARY

AUGUST 2020

Mi7 SURVEY & REPORTING PLATFORM

The Institute of Positive Education (IPE) has partnered with Resilient Youth Australia (RYA) to develop and deploy the Mi7 Survey and Survey Reporting Portal to survey and report on student and teacher/staff wellbeing. The Mi7 Survey and Survey Reporting Portal are hosted on RYA's platform and the survey data is stored on RYA's secure AWS servers.

The survey data is owned solely by IPE, but both IPE and RYA have access to such data. Specifically, IPE has access to aggregated survey responses, which is the same data that a client school or agency sees.

Given the Mi7 Survey and Survey Reporting Portal are hosted on RYA's platform, RYA's Data Policy and IT Security policy are outlined in detail in this document.

SERVER SECURITY

The RYA platform, which hosts the Mi7 Survey and Survey Reporting Portal, incorporates a dedicated instance on a dedicated Amazon account (Amazon Web Services or AWS) which features a state of-the-art cloud-based server management system.

RYA maintains its own database solution akin to a hub and spoke model. If there is any risk of a solution or database being compromised this is limited only to the single customer instance.

Features of a dedicated AWS instance include:

- Direct control over the location for the database (selected dedicated server instance in Sydney);
- The solution sitting in its own database, on its on dedicated AWS server, selected in Sydney;
- State-of-the-art firewalls;
- The database and the solution will only be accessible on demand with 1024- bit encryption;
- Access will be locked down, with single IP access only if required from the RYA office.

This system is preferable to other cloud-based Software-As-A-Service (SAAS) CRM Solutions, as these SAAS solutions have a significant number of clients sitting in the same database and server. This increases the risk of data compromisation and provides an ability for hackers to potentially gain access to the entire solution and all data for all customers in the database.

© Copyright 2020 Institute of Positive Education. All Rights Reserved.

APPLICATION SECURITY

Within the RYA solution user access is strictly maintained and based upon a logical hierarchy of data access based upon roles and requirements for staff.

Security features for access to the application include:

- All access to the system is done via industry secure socket layer (SSL) using TLS 1.2 [ensuring that all user access in encrypted];
- Named User access for each user;
- User access can be disabled instantly, and/or expiring on a predefined set date;
- Minimum password complexity requirements set for each user;
- 2 Factor Authentication for all users;
- Brute force lockout – IP Access is temporarily restricted after a set number of failed login attempts;
- Customer access limited to a small set of selected data for their own clients on a need-to-know basis;
- Bank Account details for the payments engine will be not be stored in the same database with the main customer information.

BACKUPS & DRP

RYA maintains a rigorous and detailed set of Disaster Recovery Plans (DRP) and data backups. As a general rule, all RYA instances, including IPE data, are backed up on a daily basis, with daily backups kept for six months and monthly beyond that. Backups are maintained in two locations – the main server location and a secondary remote backup with AWS.

An AWS dedicated server will [at a minimum] include a daily database snapshot. In addition, a secondary backup will be maintained in a separate selected data centre in Sydney.

In the event of a disaster the procedure is to recover the latest snapshot of the database that is available and engage a backup instance in the secondary data centre.

© Copyright 2020 Institute of Positive Education. All Rights Reserved.