Data Privacy & Security

May 2019

Approved by Massachusetts Student Data Privacy Agreement (May 2019) and Student Privacy Pledge (May 2019)

Risk-Eraser provides security for all its software (EDUCATA™, Goal Seeker™) through its underlying architecture, residing with WorldAPP. Below, we provide the specific details of our security measures. Any changes to the policies described in this document will be communicated to our users by email, and the document amended accordingly; logging on following notification of changes will be taken as an acceptance of the changes.

1. WorldAPP IT

WorldAPP IT is the primary Information Security department at WorldAPP, and is responsible for policy management, implementation, compliance and audit. Policies are reviewed on an annual basis in coordination with the COOs office and department heads. For regulatory change policies, please refer to the regulatory change management document.

The following defines information security requirements for WorldAPP.

All departments interfacing with client data must comply with the following policies and procedures. These departments include:

- Technical Support
- Client Services
- Development
- Production Regular policy compliance reviews and unscheduled spot checks with escalating reprimands ensure a high rate of compliance.

2. Physical security administration

- Data collected through Extreme Form and Key Survey (which support the Educata and Goal Seeker platforms) is co-located on servers at Savvis, a state-of-the-art storage facility with the latest in redundant power, environmental control and networking technology.

• Trained professionals safeguard the security of the Extreme Form and Key Survey network and equipment by staffing this facility around the clock. All building and environmental alarms are monitored 24 hours a day, 365 days a year. Security includes three Layers of RFID (Remote Frequency Identification) Technology to enter and leave the facility.

• Additional onsite security includes: closed circuit video monitoring (both inside and out), alarmed doors with secure key card access (requiring photo identification), man-trap restricted access to the data floor and secure locking equipment enclosures.

• Industrial strength, dedicated rack mount servers, feature multiple processors, redundant power supplies, redundant network cards and SCSI Raid 1 mirroring hard drives.

3. Security for data generated from WorldAPP forms

Customer data storage is restricted to the data center unless written permission is obtained from the client.

Customer data resides securely on Database servers behind multiple firewalls, accessible only by using the Key Survey application. Access to data, customer information and system administration (through the application and API) is limited by username and password and administrative privileges. For application administrators to access user accounts, such access must be granted explicitly by the account owner.

Under no circumstances is student or user data ever sold.

When working with WorldAPP SaaS data collection platform, all data in transit is encrypted using the VeriSign 256 bit encryption. Additionally, if the survey includes sensitive data or PII, users may employ our 'Secure Connection' feature; applying the VeriSign 256 bit in transit encryption to the survey and the data it collects. Key Survey is an official licensee of the distinguished TRUSTe Privacy Seal Program and certified by the EU Safe Harbor Privacy Program, with endorsement to securely host consumer data from any country.

For SaaS Work-Group accounts there is an additional option to encrypt data at rest. If this option is activated, Auto-filled information and all responses will be encrypted inside the database with AES-256 bits key length algorithm.

In the event of a data breach, contact administrators for the software will be notified with the details and support provided if necessary, including help with recovery.

4. Data backups and access

Backups are done by WorldAPP itself and are not accessible by customers directly and are kept by WorldAPP for recovery or troubleshooting purposes only.

WorldApp Platform is hosted on a clustered virtualized Oracle-based environment with up to 16 core and 192GB of RAM per a blade server on the back-end. For the minimum hardware requirements to a self-hosted application instance, please refer to:

http://docs.worldapp.com/collateral/Technical_requirements.pdf

5. WorldAPP's reputation with other clients

WorldAPP is an internationally recognized leader in the software industry, providing dozens of companies with a platform to collect data and chart patterns. Because of the robustness of their software, very large companies, requiring secure data solutions, have entrusted them, including MetLife, IBM, Aetna, Novartis, Deloitte, and several banks and universities.

Should WorldApp be acquired by another company, all protections and policies indicated in this document would apply for the terms of the software contract. Any potential modifications to the protections and policies of this document would be discussed with the software administrator for the school and only implemented if agreed upon by this administrator, and consistent with the policies described herein.

6. Educata and Goal Seeker specifics

Both the Educata and Goal Seeker platforms include additional HIPAA/FERPA compliance by:

- only using the first name and last initial of all students and staff
- including no information about student or staff addresses, telephone numbers or emails
- using data systems with no information about school name or location
- Email correspondence concerning data or software issues, with either our tech support team or Dr. Marc Hauser, are strictly confidential.

Educata and Goal Seeker software platforms have no advertising engines, and thus, neither students nor staff are ever presented with advertisements.

Student data is never sold.

7. Data confidentiality and access

All of the data collected by a school with either Educata or Goal Seeker software is strictly the property of the school. Risk-Eraser doesn't collect any additional data beyond what is collected and stored by a school. All changes to the data collected by a school, including student records, are made by the school and not by Risk-Eraser. It is thus the prerogative of the school to decide who is given access to the data, including students, parents, related services, and consultants.

Risk-Eraser will provide support to the school in facilitating access to the data, including risks, to whomever requests such data. Risk-Eraser staff will only use the data generated from Educata or Goal Seeker if either the school requests consultation by Risk-Eraser staff or Risk-Eraser requests access for analysis, using de-identified data. In the latter case, Risk-Eraser will only use de-identified data if permission is granted by the school. In no circumstances is the data ever sold or shared with third parties.

When the software contract is terminated, the school is responsible for exporting any data they wish to keep. Within no more than 30 days of the contract's termination, Risk-Eraser will delete all of the student personal information associated with either Educata or Goal Seeker platforms.