FIT Tracking Solutions
Privacy Document

Public Document – Version 2.0

Contents

Introduction

Alcea Technologies understands that customers place a great deal of trust in the services that we provide. Our services provide access to private customer data and it is our responsibility to make sure that this data is kept safe and confidential.

In addition to providing a safe and secure infrastructure, it is imperative that our employees are properly vetted and that they understand their obligations to all customers. This document outlines our privacy policy and the procedures in place to protect customer data.

Commitment to Privacy

Alcea is committed to the privacy of your data! We take pride in knowing that we have never had any data lost or stolen, with 20 years of service. Outlined below are the precautions we feel are necessary to continue this success.

Infrastructure Security: Our servers are provided to us by IBM Softlayer, which is one of the top data centers in the world with numerous fully compliant and audited locations around the world. Please see our Security Precautions document for further information on Softlayer and all the precautions our team takes to secure your information.

Limited Access: We've always limited direct access to customer servers, to our most senior employees who are trained and familiar with the configurations of servers, backups and protocols for dealing with customer information.

Vetting: Except for our web developers, who have absolutely no access to customer data, all our staff have Government of Canada Security clearance to Secret level. The company is facility cleared to Secret which entails several key factors on how we manage our security files and information. Most of that data is online. We are very selective about the employees we choose and rely on previous relationships of employees with potential candidates.

Legal: Every employee who works with Alcea fills out an employee contract which includes the following: "You agree not to disclose any confidential, classified or sensitive information, (either about Alcea or its clients) without the prior written approval of Alcea. You waive all rights, including intellectual property rights and moral rights under the copyright act (Canada), in respect of the deliverables on this project."

Purging: Once a customer decides to discontinue our services, we delete all their data immediately, within an agreed upon time. If the customer wishes, all data is archived and sent to them as directed.

Lost credentials and archives of data: When a customer loses access to their system or requests an archive or backup, contact to an administrator for that company or senior employee must be made. In addition, an email from the company domain must be accepted in addition to any phone calls.

Data Retention

All data is owned by the company licensing the product. If a hosted customer wishes to cancel their service at any time, we would simply need to archive the current system and transfer the data to them. In addition, this archive could be opened by the customer as a demo at a later if needed. The software also includes an export utility which can be used to output the data in CSV (Excel) or XML format.

Legal Requests for Data

Our customers trust us to keep their data safe, secure and private. Maintaining that trust is very important to us and we offer multiple geographic locations for you to store your data. We feel that the following guidelines are a fair compromise between the need for privacy and the need for justice:

- We will notify all tool administrators and provided contacts about any requests for system information, unless prohibited from doing so by law or court order.
- We will not disclose any private information, without a valid court order or search warrant from the country where the data is stored.