TRACER MANAGEMENT SYSTEMS LTD T/A Joblogic

Joblogic Server and Data Security

This policy was last updated on Tuesday 15th May 2018

At Joblogic we take data security very seriously. We know your data is precious and as custodians of that data we will do everything we can to keep it safe. We have invested heavily in world class infrastructure to protect your data.
This document explains how we store your Joblogic data and secure it to prevent customer theft, damage or loss.

System Access

As a subscriber to Joblogic, you own your data. You have control over inviting colleagues and customers to use the software and access your data. You also have control over the level of access and permissions that you give to them. Access to Joblogic is controlled by a username and password. If you think that your own security may have been breached it is essential that you notify us immediately using priority@joblogic.com or calling us on 0800 326 5561. The main subscriber can also revoke access to any accounts from within the software. It is essential that you do this when people leave your company.

Data Centre

The Joblogic application is hosted using Microsoft's World Class Azure Cloud. The nature of this type of hosting is Platform-as-a-Service (PAAS) explained here https://azure.microsoft.com/en-us/overview/what-is-paas/.

Location

At the time of writing the application and data are hosted in the UK South. Their data centres are ISO27001 Certified for data security. Click here to read more about their certification https://azure.microsoft.com/en-gb/blog/microsoft-azure-leads-the-industry-in-iso-certifications/

Data Encryption

Data is protected both in transit and at rest using https encryption.

Microsoft Azure Security

This website details the levels of security and certification provided by our hosting partner Microsoft.

https://azure.microsoft.com/en-gb/support/trust-center/

Mobile data

For the Joblogic Mobile Offline App (iOS and Android) data is stored locally and can only be accessed using the App which is protected by the username and password for the App. When in transit the data is encrypted using https. The data itself on the device is not encrypted, however a person of malicious intent would have to circumvent the Google or iOS security policies in order to access the data. Our App does not store any credit card details.

We don't store your debit/credit card information.

All our payments are processed through Stripe https://stripe.com/gb They are a PCI Service Provider Level 1 organisation - the most stringent certification level available in the payment industry.

Using Stripe means we don't need to store your payment card details, they are sent encrypted direct to Stripe, we don't store them anywhere.

You can read more about security at Stripe here: https://stripe.com/docs/security/stripe

Penetration Testing

Joblogic uses a 3rd party CREST accredited security company to provide an annual penetration test of our infrastructure. Any items arising from the pen test report are prioritised and actioned by our development team under the supervision of our Chief Technical Officer.

User Permissions

Subscribers to Joblogic can invite their colleagues to use the system.

Reporting security issues

Any security issues or concerns can be reported to us by telephone 0800 326 5561 or by email priority@joblogic.com

Security Board

Joblogic operates a security board where any security issues are escalated to senior management. Management will review the nature of the issue, decide the priority and implement any action required to provide a resolution. This includes our obligation to report any breach of personal data to the ICO within 72 hours.

ISO27001 for Data Protection

At the time of writing we have started our own journey to become 270001 accredited for data security. We have started to build our own Information Security Management System (ISMS) and expect to achieve accreditation by 2019.