recruitive

HM Government

G-Cloud

CYBER ESSENTIALS CERTIFIED

ISO

Recruitive Security

Cyber Security & Data Protection Overview

About Recruitive

Recruitive has been synonymous with Recruitment Software since 2004. We are a market-leading supplier of innovative End to End Recruitment Solutions. We have experience in the design of careers websites, recruitment agency websites and job boards since 2001.

We provide HR Professionals, Recruiters and Hiring teams with innovative, cloud-based technology aimed at streamlining the recruitment process, making it quicker and easier to recruit, whilst significantly reducing the time to hire and associated costs. As early pioneers of multi-job posting technology, our expertise extended into candidate management, CV parsing and scoring, and search capabilities right through to candidate onboarding.

In April 2019 the business was acquired and Recruitive became a wholly-owned subsidiary of SaaS Holdings Limited. We support continued investment into ongoing Research and Development in order to remain ahead of the technology curve. Our end-to-end solutions also incorporate the front-end candidate attraction capabilities of careers websites, built and designed by our in-house design specialists.

This enables us to not only deliver award-winning back-end candidate management solutions for clients but also provide beautifully designed front-end career and campaign websites to attract the best candidate talent. As a result, we are one of the few providers in the market that can deliver a complete end-to-end solution.

Based in Cannock, Staffordshire, we employ 33 of the friendliest and most competent staff. We remain an incredibly innovative business, always looking for better ways to enhance the recruitment software landscape.

We are a market-leading company.

Cyber Security and Data Protection Overview

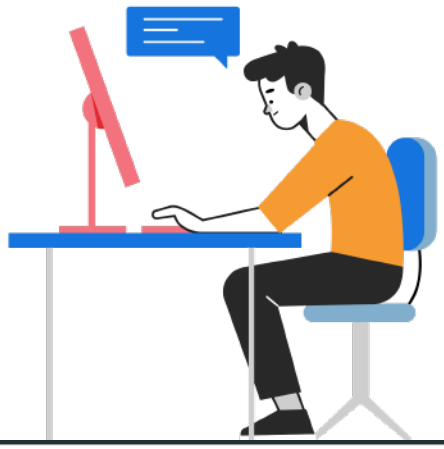
The following document describes in detail the answers to many questions relating to general security, cyber security, and data protection in connection with our recruitment software and associated services.

Where is our data and servers Located?

The data and all our internet servers are held at Tier 3+ 2N data centres in Maidenhead and Slough, UK, managed by Secura and Rackspace.

How is the data transmitted securely?

All our systems operate using SSL (Secure Sockets Layer) certificates provided by our technical security partners, tsoHost and Comodo.



What are the safeguards in place to protect client information assets aside from encryption?

All data hosted in Tier 3 data centres. The server and database access can only be accessed from specified IP addresses. The facility is managed 24/7 with CCTV and biometric entry controls.
Automated, incremental, and full data backups are performed daily, and we retain a rolling backup of all data for period of 30 days. All backups are fully encrypted and stored securely on to high-capacity disks in RAID formation on a dedicated server at the data centre. They are AES-256 encrypted and all backups are held for 30 days. No removable media such as data tapes are used, and we have constant network monitoring.

* Please also review some of our related policies

How do we manage remote access to their systems & access to client data?

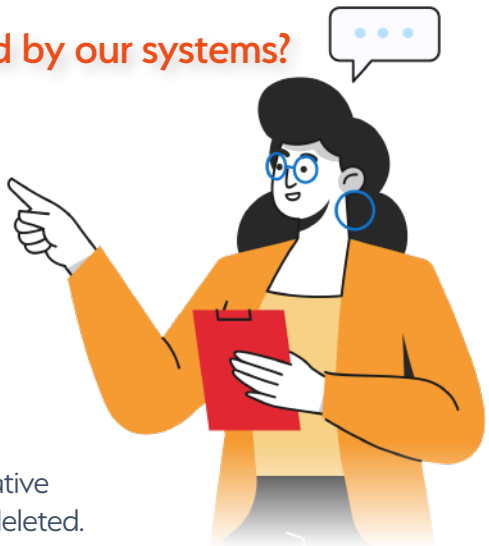
There are a team of engineers within the technical department who have access to the web and database servers. Access to these servers require a secured connection via our VPN, with access privileges controlled by a Domain Controller User Management server. SVN and SQL accounts are allocated individually, with permission access management constraints placed on each account depending on access requirements. Our user management access system tracks usage of the system logging browser / and IP location.

Is access to client data monitored and if it is, please provide details?

Our software includes log files which record access and actions by every registered user of the system. All users are logged against verification identifiers, which also record user access by date and time.

Does the client own the data stored / processed by our systems?

The collected data is the property of the company that uses our ATS. You can export it at any time.



When an agreement ends, what happens to the client's data?

Upon the end of an agreement, the data is offered to our clients either via a secure, encrypted database back up or via an alternative method of their choice. If this is declined the data is permanently deleted.

If the data is deleted, is it permanently erased?

The client data is permanently erased.

How is client data recovered in case of loss?

Automated, incremental, and full data backups are performed daily, and we retain a rolling backup of all data for period of 30 days. All backups are fully encrypted and stored securely on to high-capacity disks in RAID formation on a dedicated server at the data centre. They are AES-256 encrypted and all backups are held for 30 days. No removable media such as data tapes are used.

Will any 3rd parties have access to client data?

As standard, no third parties have access to client data. If there is an integration with a third party, then separate data processing agreements are activated.

What is our Disaster Recovery Procedure?

In the event of an incident, or if one of our servers are compromised, then data will quickly be restored from a previous, secure backup. If a server is compromised or if there is a serious hardware failure, then any system can be migrated to alternative servers or new servers can be sourced and activated at short notice. Our data centre engineers have detailed plans in place for any such incident.

Recruitive have a disaster recovery plan which is tested annually, in conjunction with our data centre engineers.

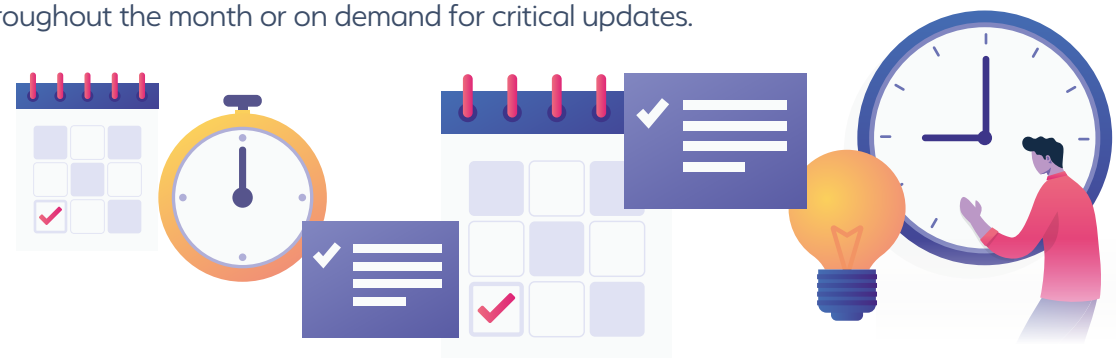
* Please also review our Disaster Recovery Policy

How often are our systems scanned for vulnerabilities?

Continuously, via the use of anti-virus and anti-malware software at server and personal level.

How do we manage system updates and upgrades?

Our servers are maintained with Microsoft Windows updates each month, which are managed by our hosting providers, Secura Node 4 and Rackspace.
ATS system updates and patches are distributed across our network of systems at scheduled milestones throughout the month or on demand for critical updates.



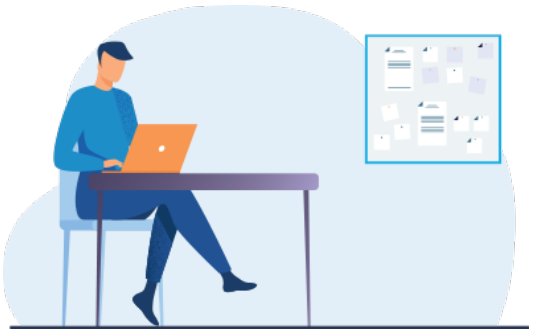
Do we undertake Penetration tests & security audits?

Our core ATS system is subject to a bi-annual Penetration test by an independent provider. Details of the Penetrations tests are confidential.

What security system monitoring processes are in place at our data centres?

The Data Centre Physical security practices & Secura Node 4 and Rackspace security procedures & processes:

- Security staff pre-vetted to BS 7858
- CCTV surveillance systems
- Regular site patrols
- Mantraps, proximity cards and biometric readers
- 4-meter-high perimeter fence
- Fill authentication and access policy control
- Biometric entry system



How do we inform customers about security issues?

Verbally and in writing, depending on the severity issue.

How do we ensure that employees are security aware?

We have security training procedures in place according to our internal security policies.

How do we ensure that the IT & Security Departments are kept current with cyber security threats & defences?

Our data centre partners have pro-active security processes in place, and we work closely with them and are in receipt of frequent security notices and bulletins.

How do we assess the knowledge of employees when it comes to cyber security?

All employees receive annual security training as part of our ongoing security policies.

Do we have cyber security liability insurance?

Yes!

How do we actively prevent data breaches?

* Please see our Data Protection Policy

How would we restore data in the event of a loss of data?

We retain secure, encrypted data back-ups of all data which are retained as incremental back-ups for a period of 30 days. The restore point for the backs-ups is 01.00am GMT. Any restorations would be from this point from the previous day.

How do we actively prevent data breaches?

* Please see our Data Protection Policy

How do we manage authorisations for internal access to client data?

* Please see our Access Control Policy

* please contact us for more infomation on this matter.

Want to know more?

Call 0345 60 00 550

Email info@recruitive.com

www.recruitive.com

recruitive