Data Controller

SPAsoft
Brewery Management Systems

The purpose of this document is to provide required information to help our customers towards GDPR compliance. As an IT company, data security is key to our very existence and as such we have always had infrastructure in place to ensure that your data is safe and secure. The following information is about where your data is stored and what we do in the background to prevent unauthorised access.
Should you have any further questions or require any further specific information, please email enquiries@spasoft.co.uk and we will do our best to help you.

Datacentre

The following information outlines specific information about our datacentre and where your data is held.

Servers

All hosted data is stored in 2 different locations, all within the U.K. and managed by IP Technology. The Primary location is the main datacentre and the second a disaster recovery site which contains a complete real time copy of ALL information in the main datacentre.
These sites are connected by an encrypted Virtual Private Network which encrypts all data before transmission. This encryption is performed at a hardware level by the border firewalls and the encryption keys are only known to technical employees. This data cannot be decoded without the encryption key whilst being transmitted across the internet.
Our Internet Service Provider is Claranet, a primarily UK based provider but their network does extend across the EU and other countries.
As with ANY provider, we cannot make any guarantee that your data may not leave the UK / EU whilst being transmitted to you.

Physical Security

Both the main Datacentre and disaster recovery sites are protected by CCTV, key fob security door access and 24/7/365 Dual Path alarm monitoring.
Key fob door access is recorded and a log can be recalled. CCTV is recorded and triggered by movement. CCTV can only be accessed by authorised personnel.
Access to the server room is only granted for maintenance, servicing and installation and as stated, access is recorded both by CCTV and secure door fob.
The alarm monitoring on our system includes but is not limited to power failures, intrusion and communication failures and is monitored at Level 4. This is equivalent to that provided to banks and other financial institutions. Monitoring is enabled both by IP and mobile network connectivity (GPRS). This ensures continuous monitoring in the event of either a fibre or GPRS failure.

Power and Connectivity

All servers are powered by intelligent "On Line" UPS units. The servers are isolated from the main power network and powered by batteries which are then constantly charged by the incoming mains network. These units will keep our systems awake for 2 hours in the event of a power failure to the Datacentre. We have a backup generator in place should any outage last longer than the capacity of the UPS units. IP Technology employees are notified by the monitoring systems in the event of a power failure.
A test of the UPS units is conducted weekly and a power failure and generator test is performed every three months.
Our Datacentre internet connectivity is provided by a dedicated fibre connection and is backed up by a redundant FTTC copper circuit which automatically fails over in the event of a fibre failure.
Our fibre connectivity is covered by a comprehensive service level agreement with a 4-hour guaranteed fix.

External Access and Virtual Server Security

All access to our hosted platforms are all granted through our internet facing firewall. We have a redundant pair configuration so that in the event of a failure, the redundant unit becomes active.

These units are kept up to date with the latest firmware and upgraded when this becomes available and has been tested. Redundancy testing is also performed on a 3-month basis.

Virtual Servers

Each of our fully hosted servers resides on one of 2 physical hosts. This is known as **Multi Tenancy**.

Each Virtual Server runs in complete isolation from any other virtual instances on the physical server. Each system runs on a “Virtual LAN” and as such all network communications are isolated to each Virtual Server. It is not possible for any data from one server to be seen by another due to this Virtual LAN configuration.

Remote Desktop Systems

Our fully hosted servers are accessed via RDP Protocol and all communications are secured and encrypted by a 256-bit encryption certificate.

Our firewall is programmed to detect port scanning and denial of service attacks and automatically blocks any traffic which it detects may be connected with this activity.

We have also recently introduced a further level of security which detects and blocks any failed logins or brute force attacks. This system automatically blocks an intruder (3 failed login attempts) for 20 minutes and then if the intrusion persists a lock for a minimum of 24 hours is put in place.

Our support team is notified of any hard or soft locks, and repeat offenders and their entire IP range is then denied access to our network permanently. This traffic does not then pass our firewall.

We have extended this to our customers who also have RDP ports open for remote access to their own servers or for us to service their systems.

For those customers who do not access their systems remotely but have ports open for us to access, your firewall / router has been configured to ONLY accept connections from our IP range in addition to the intrusion detection. The firewall blocking has been standard practice on our installation for a number of years.

On Site Data Access and Backups

IP Technology employees will only access the SPAsoft servers to perform maintenance, install operating system patches or software upgrades. This access is necessary in order for us to fulfil our contractual obligations to you as per the hosting agreement. We will always notify and log any such access should it be required.

We will only perform software upgrades upon your request and this request will be recorded in our call logging system. This call log will also contain all the details of exactly what has been performed. **THESE ARE THE ONLY CIRCUMSTANCES UNDER WHICH YOUR HOSTED SYSTEMS WILL BE ACCESSED.**

At the moment, we hold a record of all administrator passwords on our internal systems for maintenance purposes, but this can be removed at your request. As a hosted customer, you are at liberty to change any administrator access passwords at any time. You do not have to reveal this information to us but it will be required as and when maintenance is performed. Again, you are at liberty to change any password on any of your systems at any time and you DO NOT have to inform us, although this will stop us from performing any upgrade maintenance to your systems.

Backups

Backups of the entire system is performed once every 24 hours. Due to storage restrictions, we keep 2 weeks’ worth of backups and then the oldest backup is overwritten.

We will restore individual files and folders as part of your hosting contract. The backup of this system is for disaster recovery only.

Who has Access to the Hosted Platform(s)

At any time, only technical support engineers who are employed by IP Technology have access to the physical host and virtual servers. Again, this is for support, maintenance and upgrade purposes only. Any external service personnel who visit our premises to perform servicing on vital equipment (Mains Electricity or Air Conditioning for example) are accompanied by an employee of IP Technology at all times.

• **Network Security and Customer Data**

The network can only be accessed via internal terminals, 1 Remote Desktop Server and an encrypted tunnel to our DR centre. We have a password change and complexity policy on site.

Employees are only granted access to data which is pertinent to their role.

As a company we DO NOT harvest customer information and only store that which is relevant so we can carry out our contractual obligations to our customers.

Customer information will only be passed on to those parties which require it to enable us to fulfil our obligations. These include but are not limited to UPS (our chosen courier) and certain trade distributors should a direct delivery be required.

We do not currently perform any email marketing and as such that is why you will not have received any consent requests from us. Should we wish to contact you in the future to advertise any of our services by email, we will be in contact to request consent.

We DO NOT pass on any customer information or data to ANY 3rd parties for the purpose of marketing and will never do so.

We will be updating our privacy policy which can be viewed on our website at www.ip-technology.com This will be in place by May 25th.

Whilst we do not collect, process or store ANY sensitive personal information on our own internal servers or systems, our equipment may be used to do so. Whilst it is our duty to ensure that our systems are as secure as possible, if, as one of our customers, you do collect and process this type of information, you are responsible for ensuring that your own company policies are in line with the incoming GDPR regulations.

Your data security is of utmost importance to us and we are constantly reviewing and improving our internal policies to improve this where possible.

We do NOT currently undertake any penetration testing as we feel that our existing systems are robust enough to ensure that we catch any intrusion when and if they happen. However, this policy is always in review and will be updated as and when necessary.

At any point, should you wish to request a list of all the data that we hold on your business, please email nigel@spasoft.co.uk where your query will be dealt with as soon as possible.

Should you have any questions or queries regarding any aspect of this document, please email