SAAS SPECIFICATION

All the information you need to know about our SaaS Platform

01344 452778 printonlineportal.co.uk hello@printroom.co.uk

Printroom House, Downmill Road
Bracknell, Berkshire RG12 1QS

SaaS Specification

Hosting

Our service is hosted between two ISO 27001 certified, third party specialist data centres based in the UK.

For more information click here.

Redundancy

Redundancy is essential when providing a reliable service with high availability.

- Your data is replicated every eight hours to a secondary storage device.
- All disks have been setup as a RAID (Redundant Array of Independent Disks)
- Active monitoring is employed on all critical components.
- Your application is hosted on a virtual server for high availability.
- All servers are protected by redundant firewalls, switches and power supplies.
- Our composition layer is clustered which enables us to restart individual rendering servers without affecting availability.
- Redundant DNS servers for ease of mind.

Backups

We know your data is mission critical.

- Your data is replicated every eight hours to a secondary storage device.
- Your data is backed up every 24 hours. Your data can be backed up more frequently at an additional cost. For more information, please contact POP
- To protect backups from malicious attacks we create offline backups (tape) every 30 days.

Retention Policy

We retain your data as long as it is necessary and relevant for our operations. In addition, we may retain data from closed accounts to troubleshoot problems, enforce our User Agreement and take other actions permitted or required by applicable national laws. After it is no longer necessary for us to retain your data, we dispose of it in a secure manner according to our data retention and deletion policies.

We operate a GFS retention policy which is a backup rotation scheme intended for long-term archiving.

Backups are held:

- Daily up to 7 days.
- Weekly up to 4 weeks.
- Monthly up to 12 months.
- Yearly up to 3 years.

Data Recovery

Data recovery is only included in the unlikely event of a disaster. Recovery of data due to user error will be chargeable.

Disaster Recovery

Disaster Recovery Plan

Our disaster recovery plan is continuously reviewed and approved by executive management.

The disaster recovery plan contains confidential data, for this reason the document is not publicly accessible.

Plan Testing

Our disaster recovery plan is regularly tested to identify changes in the environment, include any new situations and to accommodate any altered conditions.

The plan was last tested on the 05/04/2016 and will be tested on the 05/10/2016.

Objectives

The recovery point objective is the maximum tolerable period in which data might be lost due to a disaster.

Your data can be backed up hourly or daily to meet your required recovery point objective. For more information please contact hello@printroom.co.uk

The recovery time objective is the maximum tolerable period in which normal business operations must be restored, in the event of a disaster.

The time taken to restore a system from backup depends on the size of your application and the severity of the disaster. We offer a recovery time objective of one or six working days. For more information, please contact hello@printroom.co.uk

Data protection

It is of utmost importance that your data is safe and secure.

We are registered with the Information Commissioner's Office in compliance with The Data Protection Act 1998 and our certificate of registration can be found here.

We utilise some of the most advanced technologies for Internet security available today, for example:

- When you access your application using a supported web browser, Secure Socket Layer (SSL) technology can be applied to protect your information using both server authentication and data encryption.
- Your application is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders.
- We backup multiple copies of your data to ensure your data will not be lost.

For more information on how we keep your data secure please see our security, backup and data retention policy.

Security

Audits

We contract with independent specialist security companies to conduct 3rd party audits and penetration tests to improve security controls and processes.

Our service was last audited in August, 2016

For security reasons the audit is not publicly accessible however, an assessment can be found by clicking here.

Security assessments commissioned by the client are permitted however, due to the different types of security assessments we would require a plan test and scope before approving.

Physical security

Our service is hosted between two third party specialist hosting facilities, designed to run 24x7x365 and employs various measures to help protect operations from physical intrusion.

These data centres comply with industry standards such as ISO 27001.

Only authorised persons are allowed to access the data centres.

Access lists are maintained between two third party specialist hosting facilities. Additional access can only be granted by a director. Access lists are periodically checked with the 3rd party to verify accuracy.

Firewalls

Physical and software firewalls are in place to control incoming and outgoing network traffic.

Antivirus

Antivirus software is installed to ensure any malicious files are removed when detected.

Virus defintions are automatically updated every 24 hours.

Scanning configuration:

- Files are scanned on access.
- Critical areas are scanned daily out of hours.
- Full scans run weekly out of hours.

Denial of Service (DoS) Attacks

Our environment has a defence system to to block network attacks including port scanning, denial-of-service attacks, buffer-overrun attacks and other remote malicious actions taken against the programs and services working with the network.

Security Updates

Security updates are applied to protect systems from known vulnerabilities.

Updates are tested in a separate test environment before release.

Our software is periodically checked to ensure security updates are applied in a timely manner.

Encryption

Secure Socket Layer (SSL) technology can be applied to encrypt traffic between the application and end user. To setup SSL please contact hello@printroom.co.uk

Stored data is not encrypted at present.

Access

Remote access to production application systems are only provided to our support and development team.

RDP is restricted by IP and valid login credentials are required.

Computer Security Incident Response Team (CSIRT)

The CSIRT objective is to minimise and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening.

In the event of a security breach, all clients that may have been affected will be contacted so they can judge appropriate response including informing the Metropolitan Police if necessary.

Monitoring

To provide a reliable service we automatically monitor numerous critical components, these include:

- Memory
- Storage
- Bandwidth
- CPU utilisation
- Availability
- Response times

Our monitoring services automatically notify our technical team via email or SMS.

The availability of your site is automatically monitored every 30 seconds.

We also manually check the environment to ensure our monitoring services are running accordingly.