Information Security & Business Continuity

Last revised: March 2019

To ensure service availability we have identified and implemented the following measures:

Physical security
Servers and other network equipment are housed in locked cabinets. The server cabinet is housed in a locked computer room. The room is within our office environment and is protected by physical access controls. A dedicated air conditioning unit serves the room.

This facility incorporates the following systems to ensure maximum resilience and service availability:

- the building is protected externally by recorded 24/7 CCTV coverage.
- only authorised staff have physical access to the computer room.
- security engineers monitor both managed devices and external threats.
- server operating systems are hardened to best practice standards.
- security patches are applied as new threats emerge.
- managed antivirus service is powered by Sophos.
- fully managed firewalls.
- fire detection and alarm system.
- security access system.

Servers
Servers are protected by windows firewall with advanced security. The firewall is configured to block all traffic except on specific ports. We apply all critical and important security patches on a weekly basis.

Data backups
Weekly backup to disk held off site at a secure location. Daily overnight backups on a 5 day revolving cycle. All backups are encrypted.

Information security
All data is stored on our servers. Data is encrypted. No client data is transported from our offices.

Printed confidential information and computer media are disposed of in accordance with EN15713.

We publish our information security guidelines and deliver in-house training to our staff.

We are Cyber Essentials Plus accredited, which we operate in conjunction with best practice guidelines.

> Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks. Certification gives you peace of mind that your defences will protect against the vast majority of common cyber attacks simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place. If you would like to bid for central government contracts which

involve handling sensitive and personal information or the provision of certain technical products and services, you will require Cyber Essentials Certification.

Any suspected breaches of our information security are escalated to the appropriate person for investigation to determine the scope, severity and corrective action. Any corrective action required would be notified to all employees with immediate effect. If appropriate, breaches would be notified to our stakeholders.

Client data
All data held on our servers is at all times our property, unless contractually stated. Any action applied to data is performed by Splitz authorised personnel only. Upon contract termination access to client data is disabled and subsequently archived in accordance with our data retention policy, or returned to the relevant commissioner.

Service
Access to the server is over TLS 1.2 using AES 256 bit encryption. Our developers are well versed in developing secure code as this is critical to the nature of the service we provide.

Recruitment
We operate a rigorous recruitment process. We conduct all applicable background checks and require satisfactory employment references.

Disaster recovery
Our team of multi-skilled and multi-disciplined personnel can perform in a number of functions within the business providing cover for illness, accident or disaster with defined escalation procedures in place.

We have technical solutions to enable our business to function remotely and we have a business continuity plan in place that covers our operations.

Office locations
Offices in Trowbridge house our Wiltshire support teams, finance, and support functions.
Offices in Exeter and Barnstable house our Devon support teams.
Offices in Gloucester house our Gloucestershire support team.

Access to the premises is controlled by access control systems.