SchemeServe

Business Continuity, Disaster Recovery and Information Security Statement

At SchemeServe, we recognise that our customers rely on us to provide software solutions that are effective, but also resilient. Whilst we are confident in our ability to deliver our services without interruption, we acknowledge that the unexpected can happen and must be planned for. Business threats such as that posed by cybercrime are very real and we pride ourselves in being proactive in identifying and mitigating against these threats.

The following information outlines our approach to Business Continuity, Disaster Recovery and Information Security, summarising the plans and processes we have put in place to maximise resilience and to ensure that our customers can have complete confidence in our ability to deliver on a round-the-clock basis.

1.1 Business Continuity Aim & Objectives

As part of our commitment to Business Continuity, SchemeServe have identified an aim and set of objectives which describe and govern our approach to resilience. The Business Continuity aim is to ensure that SchemeServe continues to provide its service to its existing customers, should an adverse situation arise. The Business Continuity objectives specific to the company are:

- To safeguard the delivery of SchemeServe products and services to customers.
- To safeguard staff and the interests of SchemeServe and its customers including key stakeholders, brand, reputation and value through Business Continuity Management – a process which identifies potential risks, their impacts, builds resilience and ensures capability for an effective response, including effective Crisis Management.
- To ensure that the Directors meet their key responsibilities, ensure continual improvement of the BCMS and satisfy all applicable requirements.

1.2 Business Continuity

SchemeServe recognise that IT resilience & Disaster Recovery arrangements form only part of our broader approach to Business Continuity, which is underpinned by our Business Continuity Management System (BCMS). Business Continuity Management is a holistic management process, where we identify and acknowledge potential threats to our business and the likely impact upon our business operations should they occur. The BCMS provides a framework for building organisational resilience; detailing comprehensive and effective strategies for dealing with the identified threats, and a team which understands how to implement these and deliver a robust and effective response to any incident.

SchemeServe’s BCMS is based on the professional practices outlined in the Business Continuity Institute’s Good Practice Guidelines 2013. Our Business Continuity arrangements are laid out in our Business Continuity Plan, which is routinely exercised to ensure its relevance and to identify opportunities for improvement.

Risks are identified and assessed with regards to their likely impact on Premises, People, Resources & Suppliers (PPRS). Given the nature of SchemeServe operations, we recognise that our most potent threats are focussed on resources (including IT systems) and suppliers. Risks that we have identified and developed recovery strategies for include; a loss of servers, a loss of telecommunications capabilities, loss of key personnel, and loss of externally-hosted platforms.

As part of our BCMS, we conduct regular exercises to allow for the continuous improvement of our BC plans and to constantly improve the awareness and skills of our employees, ensuring that BC is part of ‘business as usual’. Following each exercise, we write a report to evidence the exercise and ensure any learning points are recorded and acted upon; we are happy to provide copies of these reports to our customers on request.

1.3 Disaster Recovery

As a cloud-based provider of software solutions, we recognise that our greater risks are posed by a loss of the information and/or systems that we rely upon to deliver our quality services to our customers. Our Business Impact Analysis confirms that the threat with the greatest consequences to the company is a loss of data or our systems capabilities. As such, we have ensured that our IT systems are designed with resilience in mind, to mitigate against the risk of any downtime. We also have identified Disaster Recovery response strategies to assist us in responding in the unlikely event of a serious IT incident.

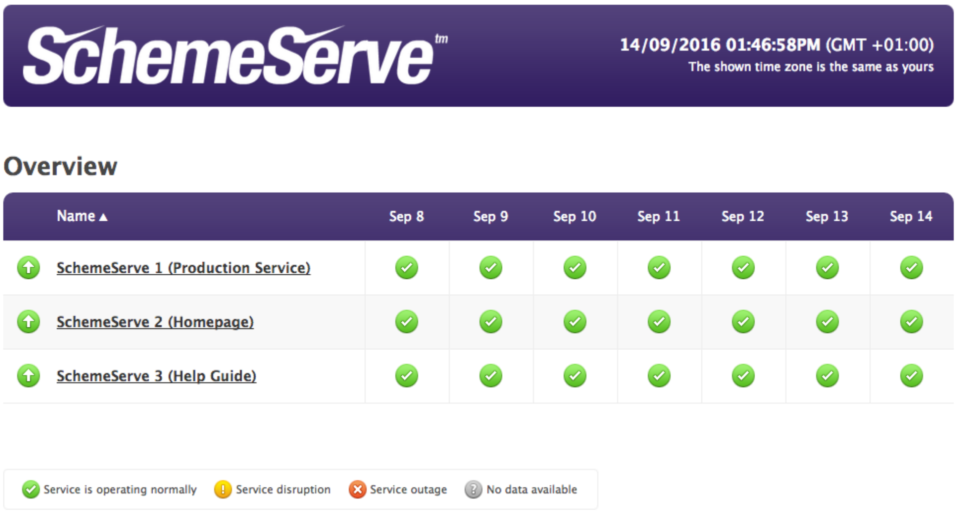
- Our data centre and servers are hosted by Rackspace, a well-respected cloud provider of resilient server solutions, who provide services to a wide range of multinational companies and public sector organisations, from Virgin Trains to the NHS. The servers are located at Rackspace's facility in London LON3; one of the United Kingdom's most advanced data centres with a 100% network uptime guarantee.

- The servers at the London data centre backs-up to a second server cluster every four hours, and is manually verified regularly to ensure its integrity.

- Verified information from the servers is backed-up at an off-site facility in the north of England, provided by Iron Mountain; globally-respected professionals in the storing, protection and management of information and assets. This ensures that our data can be recovered, either through downloading or physical transfer, on a round-the-clock basis. Information on our off-site system is stored for a period of one year. An additional standby copy of data is also held on Microsoft servers in Dublin, Cardiff, Oxford and the Netherlands to mitigate any loss of the primary and secondary server and the back-up site.

- Our Helpdesk and Sales websites provide dedicated support for our valued customers. To increase their resilience, these are hosted externally, meaning that we can continue to communicate effectively with our customers in the highly unlikely event that our servers were offline. Our dedicated telephone service adds additional resilience, ensuring that we are always within reach.

- We are so confident in our uptime that our uptime monitoring data is published on our website automatically:



SchemeServe™

14/09/2016 01:46:58PM (GMT +01:00)
The shown time zone is the same as yours

Overview

Name ▲	Sep 8	Sep 9	Sep 10	Sep 11	Sep 12	Sep 13	Sep 14
SchemeServe 1 (Production Service)	✓	✓	✓	✓	✓	✓	✓
SchemeServe 2 (Homepage)	✓	✓	✓	✓	✓	✓	✓
SchemeServe 3 (Help Guide)	✓	✓	✓	✓	✓	✓	✓

✓ Service is operating normally ! Service disruption ✕ Service outage ? No data available

1.4 Information Security

SchemeServe has designed and implemented processes and methodologies to protect ours and our customers' confidential data from unauthorized access, use, disclosure, destruction, modification or destruction.

Our data is held on servers provided by Rackspace who are certified to ISO 27001, the international standard for Information Security Management. They are also globally certified as a Level 1 PCI-DSS Service provider regarding physical security and the shared network infrastructure. Rackspace undergoes a global SAS70 Type II audit annually, a report of which can be provided on request. SchemeServe customers can therefore be rest assured that all data is handled in the strictest confidence and according to recognised, stringent security standards, with full encryption of data at all sites.

Further provisions that SchemeServe have made with regard to Information Security include:

- Licences for software used by SchemeServe staff are stored in a secure online repository at Rackspace.

- Historic, version-controlled copies of all documents are stored in a secure online repository. For convenience, printed copies of documents may be used from time-to-time but not containing sensitive data.

- Key Staff, Supplier & Customer Contact Details are recorded and kept up-to-date in our secure online document facility. Copies are maintained on local computers and in our hosted corporate e-mail and address book facility.

- Source code, design originals and staff documents are managed via version-control software maintained as part of a secure source code hosting facility. Changes cannot be made to source code without logging time-stamp, staff-member username and full source code history before and after the change. Certain documents are also managed and edited securely online.

1.5 SchemeServe & PlanB Consulting

SchemeServe developed its approach to Business Continuity in partnership with PlanB Consulting, one of Europe's leading Business Continuity consultancies.

Established in 2007 and based in Houston near Glasgow, PlanB Consulting provides full lifecycle Business Continuity services to the private, not-for-profit and public sectors. They deliver Business Continuity development and training, ISO 22301, exercises, Disaster Recovery and Incident Management support services worldwide, predominantly in the UK and Europe. They they have experience of implementing BCMS in some of the world's largest companies and across a range of industries, from logistics to financial services, and from telecommunications to building services.

PlanB Consulting helped SchemeServe produce an industry standard Business Continuity solution so customers can be assured their plans are in line with industry practice. PlanB Consulting also externally reviewed SchemeServes Disaster Recovery exercise in October 2016, confirming this was a robust test of their technical recovery actions, with learning points identified and acted upon. PlanB Consulting's experts remain available for consultation with SchemeServe, meaning we can draw upon additional support and expertise in the event of a significant incident.