SCHEDULE 2

Service Level Agreement

GENERAL

1. Definitions

All terms defined in this SLA shall have the meaning set out in the Terms and Conditions, unless defined otherwise below.

'Availability'	means that the Solution shall be available via the Internet 99.5% during Business Hours measured annually from the go live date;
'Bug'	means an unwanted or unintended malfunction of the Solution that can be reproduced which does not affect the availability of the Solution;
'Business Day'	means Monday to Friday excluding any national holiday in the UK;
'Business Hours'	means 9 am – 5.30 pm;
'Disaster'	means the hosting centre where the Solution is hosted becomes unusable, with little chance of a short term recovery;
'**Emergency Maintenance**'	means maintenance, Upgrades, updates, repairs to hardware and software related to resolving immediate problems causing instability in the Solution;
'Incident'	means a malfunction of the Solution which is not a Bug, whose root cause is found in the Services, network, hardware or third party software components;
'Patch'	means a bug fix, performance or SLA improvement;
'Planned Maintenance'	means maintenance, Upgrades, updates, installation of new versions and repairs which are non-critical and not urgent, to hardware and software;
'Release'	means a modification in the functionality of the Solution which results in a change in the version number as set out in the SLA;
'Upgrades'	means any new or updated applications services or tools (including any software programmes) made available by the Company as part of the Solution during the Term.

HOSTING SERVICES

Hosting Services shall include hosting of the Solution together with related components and Customer owned content as set out below.

2. Solution Availability

2.1 Availability

The Company will take all appropriate measures in terms of redundancy, monitoring and platform management to provide Availability of the Solution.
The events set out in section 7 of this SLA and Planned Maintenance shall be excluded from the calculation of Availability.

3. Security Infrastructure

The following infrastructure and security is provided at the Company's data centres in the United Kingdom with 1 and 1 Internet Limited. The Company reserves the right to change the data centre during the Term, provided that any new data centre provides at least the same level of services and security as the current data centre.

3.1 Data Centre Network

The Company provides web servers, application servers, database servers and physical data storage in which data is stored in a redundant multi-drive configuration that provides the necessary software to host the Solution and Services. Web-based application use Secure HTTP (HTTPS) to protect data transmissions over the Internet.

3.2 Security and Environment

The Hosting Services are provided in a secure, limited access environment. There is an uninterrupted power source, climate control and the data centre is hardened against natural disaster. In case there are reasonable doubts about the security of the data centre, the Customer may instruct an independent third party to check the security systems at the data centre at its own cost and provided that the Customer reimburses the Company for all costs it incurs in assisting with such inspection, in particular any fees that the Company must pay to the data centre. Access to the data centre infrastructure will be at the sole discretion of 1 and 1 Internet Limited.

Access to the data centre is limited to specific staff members and a select number of production support specialists and information technology specialists, who may only access the data centre to perform routine maintenance and Upgrades.

3.3 Monitoring

The Company provides the following 24 x 7 monitoring:

- server hardware;
- system availability;
- network infrastructure;
- operating systems services (WWW, SMTP, SQL);
- application availability.

All Company servers are protected by Firewall appliances. All servers accessible from the Internet are located in a DMZ, servers storing Customer data are located within the protected network. All servers are installed with the latest security patches and are hardened as per manufacturer's recommendations.

3.4 System Backup

The Company ensures that data is protected using backup to disk. Hosting company guarantees daily backups of the whole system. The Company performs a full database backup to disk once every month. These incremental backups will be retained for 12 months in case the Customer need to retrieve earlier data. Additional backups are performed by the Company prior to Releases.

MAINTENANCE AND SUPPORT SERVICES

Maintenance and Support Services shall include maintenance of the Solution and Customer platform including corrective maintenance and enhancements and a customer support service for the Solution and Customer platform as set out below.

4. Support Services

4.1 Scope of Support Services

Maintenance and Support Services shall not be provided for issues arising from (i) modifications, alteration or configuration of any of the Services by the Customer or a third party that have not been authorised in writing by the Company and/or (ii) technology or IPR that has not been provided by the Company pursuant to the Agreement.

4.2 Problem Notification

The Company provides support services from a support centre which is available to named support users. Support Services are provided in English.

Problems may be reported to the support centre by email.

4.3 Problem Acknowledgement

Upon receipt of a problem notification the Company shall respond to the Customer, within the time frame set out in sections 4 and 5 of this SLA as applicable, based on the severity and type of problem. Such response shall specify the severity level and type of problem.

4.4 Standard Support

The Company provides support for the Solution and Services during Business Hours on Business Days in English. This includes appropriate project management to ensure proper operation of the Services and Solution.

4.5 Problem Severity Classification

Severity	Description
High	A problem is classified as high if: • the Solution is not available to the Customer and candidates; or • the Customer cannot log in, for reasons other than account suspension or providing incorrect logon details; or • there appear to be serious performance or access problems; or • there are other problems which result in loss of availability of the Solution.
Medium	A problem is classified as medium if: • part of the Solution is unavailable but a workaround is possible; or • other features are not operational; and the availability of the Solution is not affected.
Low	A problem is classified as low if: • there are visual or behavioural inconsistencies in the Solution that make the usage uncomfortable but do not prevent the use of the Solution or access to sensitive pages; or • there are visual or behavioural inconsistencies in the Solution but use of Key application Features nor access to sensitive pages is not prevented; or • there is any other problem that does not fall into any other category within the severities High, Medium or Low.

Response and Target Resolution Times

Severity	Response Time	Target Resolution Time for Incidents		Target Resolution Time for Bugs	
		Temporary work around	**Permanent**	**Temporary work around**	**Permanent**
High	Within 8 Business Hours	8 Business Hours	2 Business Days	2 Business Days	3 Business Days
Medium	Within 2 Business Days	2 Business Days	2 Business Days	**Next Release**	
Low	Within 3 Business Day	3 Business Days	5 Business Days	**Next Release**	

Downtime will begin to be measured upon receipt by the Company of the Customer's notification of the problem.

5. Maintenance

5.1 Upgrades

The Company will provide the Customer with Upgrades of existing modules at no additional cost, when these are offered generally to its customers.

5.2 Planned Maintenance

The Company usually carries out Planned Maintenance in the maintenance windows set out below. If Planned Maintenance is to be performed outside of these windows the Company shall give the Customer at least 48 hours prior notice.

Normal Patch	
Deployment window	during Business Hours
Deployment schedule	Tuesdays
Interruption of service	Usually 1 hour

Maximum interruption of service	4 hours
Upfront Notice Period	Usually 2 days

5.3 Emergency Maintenance

The Company shall where possible, provide the Customer with prior notice of Emergency Maintenance. However, work may commence at any time and shall continue until completed. The Company shall attempt, but cannot guarantee scheduling Emergency Maintenance during non-Business Hours.

5.4 Patches

The Solution and Services will be patched regularly for performance and security, after such patches are regression tests with the Solution and Services to ensure continued compatibility.

6. Customer's Obligations

The Customer has the following obligations under this SLA:

- to provide access to a computer system capable of running the TCP/IP network protocol and an Internet web browser and uses a web browser that supports JavaScript;
- to provide all suitable hardware and software and telecommunications equipment required for accessing the Solution and Services;
- responsibility for the network connection between the Company's hosting centres and the Customer's premises (backend) connection to a telecommunications network;
- to inform the Company without delay of any problems with the Solution or Services;
- to purchase upgrades for its own software, if necessary, for the error free operation of its own software with the Solution;
- to check its systems for the most commonly known worms and viruses;
- to have a current virus scanner installed for each Customer system accessing the Solution.

7. Limitation of Liability

The Company shall not be liable for, and shall have no obligation to fix, any errors, Incidents, problems or Bugs or any lack of availability of the Solution or Services caused by the following:

- any breach of the Customer's obligations set out in section 6 above;
- use of the Solution on a system not supported by the Company or specifically agreed in the Implementation Plan;
- unavailability of telecommunications;
- faults or omission of ISPs;
- any lack of connectivity caused by a third party;
- any Bugs or defects in any third party software that interacts with the Customer's data once it leaves the Company's hosting centres;
- any denial of service attacks, network floods and hacking;
- interconnection of the Solution with other software products not supplied by the Company except as expressly agreed in the Implementation Plan;
- any DNS issues not within the direct control of the Company i.e. a fault on the Customer's network or own equipment configuration;
- problems or errors that occur while the Company is waiting for the Customer to provide information to enable it to rectify a fault or restore services;
- faults caused by the Customer's management or connection to the Solution;
- the Customer failing to take part in training offered by the Company, necessary for use of the Solution;
- Force Majeure.