This document has been redacted to remove any commercially sensitive information and is now classified as DCC Public.

Should you have any queries, please contact Commercial@SmartDCC.co.uk

SCHEDULE 7

SECURITY REQUIREMENTS

1. GENERAL SECURITY REQUIREMENTS

1.1 The Contractor shall:-

1.1.1 take all such steps as are required in accordance with Good Industry Practice, or as are otherwise agreed between the Parties, to ensure the security of the Contractor and the Contractor Systems;

1.1.2 ensure the security of Contractor Personnel and the Sites in accordance with Good Industry Practice; and

1.1.3 ensure the security of all Contractor Persons (including their Systems, solutions and services) in accordance with Good Industry Practice in connection with the provision of the Services.

1.2 The Contractor shall provide a reasonable level of access to the DCC to any member of the Contractor Personnel for the purpose of designing, implementing and managing security.

1.3 The Contractor shall act in accordance with Good Industry Practice in the day to day operation of any Contractor System holding, transferring or processing DCC Data and any Contractor System that could directly or indirectly have an impact on that DCC Data and shall ensure that any such DCC Data remains under the effective control of the Contractor at all times.

1.4 The Contractor shall ensure the up to date maintenance of a security policy (the "**Security Policy**") and Security Management Plan relating to the operation of its own organisation and the systems, and on request from the DCC shall supply to the DCC the current version of such documents as soon as practicable. The Security Policy shall be a document that establishes the Supplier expectations of security, the security objectives or a method for setting security objectives, measures to identify and mitigate risks, the classification and handling of information, and senior management responsibilities and support of security within the Supplier.

2. SECURITY MANAGEMENT PLAN

2.1 Within sixty (60) Business Days of the Commencement Date, the Contractor shall prepare and submit to the DCC for approval a fully developed, complete and up-to-date draft Security Management Plan. The Security Management Plan shall be a document, or collection of documents, detailing how security will be assured for the provision of the Services, the Contractor Solution and for the DCC Data. The Security Management Plan can make reference to existing Contractor security policies, practices and an information security management system or new security policies, practices and information security management systems that will be introduced for the Services.

2.2 The Security Management Plan shall:-

2.2.1 be consistent with the security requirements stated in Schedule 3 (*DCC Requirements*);

2.2.2 include provision for the implementation of control requirements within timescales agreed with the DCC that are identified as a result of any security audit undertaken in accordance with Schedule 3 (*DCC Requirements*);

2.2.3 comply with the Security Controls and describe how such compliance will be achieved;

2.2.4 take account of and, to the extent applicable to the Contractor Solution and the provision of the Services, be consistent with the security requirements set out in Section G of the SEC;

2.2.5 be consistent with, and include all the elements of a plan prepared in accordance with, Good Industry Practice;

2.2.6 set out how the Contractor shall ensure that the Services are the subject of robust and appropriate security management systems;

2.2.7 be consistent with the quality standards set out in Schedule 6 (*Standards*) including any such standards that relate specifically to security;

2.2.8 be otherwise consistent with the requirements of the Agreement;

2.2.9 identify a senior manager appointed by the Contractor who is responsible for security and who has formally approved the Security Management Plan;

2.2.10 include the relevant contact details of the Contractor and the relevant Contractor Personnel to be used by the DCC to coordinate security incident response and other operational security considerations with the Contractor;

2.2.11 detail the process for managing any security risks, including those from Contractor Persons (including their respective Systems, solutions and services) in respect of their involvement in the provision of the Services;

2.2.12 unless otherwise specified by the DCC in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the DCC Premises, Sites, the Contractor System and DCC Data to the extent used by the DCC or the Contractor in connection with this Agreement or in connection with any System that could directly or indirectly have an impact on the DCC Data, the DCC Environment and/or the Services; and

2.2.13 set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the provision of the Services and the Contractor Solution comply with the requirements set out in this Schedule 7.

2.3 As soon as reasonably practicable after receipt of the draft Security Management Plan from the Contractor, the DCC shall notify the Contractor if it (acting reasonably) considers that the draft does not comply with any of the requirements set out in this Schedule 7 (each for the purposes of this Schedule 7, a "**non-conformity**").

2.4 By no later than ten (10) Business Days after receipt of a notice from the DCC under Paragraph 2.3, the Contractor shall:-

2.4.1 make any amendments to the Security Management Plan that are necessary to address the non-conformities notified by the DCC under Paragraph 2.3; and

2.4.2 re-submit the revised Security Management Plan to the DCC for approval.

2.5 As soon as reasonably practicable after receipt of the revised Security Management Plan from the Contractor, the DCC shall notify the Contractor of any new or outstanding non-conformities.

2.6 The process in Paragraphs 2.4 and 2.5 will then be repeated until the DCC notifies the Contractor that the Security Management Plan is approved. Any Dispute relating to the existence of non-conformities in the Security Management Plan shall be referred to the Dispute Resolution Procedure. Once approved by the DCC, the Contractor shall ensure that:-

2.6.1 it implements the Security Management Plan;

2.6.2 the Services are carried out in compliance with the Security Management Plan;

2.6.3 the Contractor Solution is operated in accordance with the Security Management Plan.

2.7 The Contractor acknowledges and accepts that the DCC's approval shall not act as an endorsement of the Security Management Plan and shall not relieve the Contractor of its responsibility for ensuring that the Services are provided, and its obligations performed, in accordance with the requirements of this Agreement.

2.8 The Contractor shall, at its own cost, review and update the Security Management Plan so as to ensure that it accurately reflects:-

2.8.1 the then current Contractor Solution and Services and the manner in which they are provided, and otherwise continues to comply with the requirements of this Schedule 7;

2.8.2 emerging changes in Good Industry Practice;

2.8.3 any change or proposed change to the Services and/or associated processes and the Contractor System;

2.8.4 any new perceived or changed security threats; and

2.8.5 any reasonable change in requirement requested by the DCC.

2.9 The Contractor shall carry out the review described in Paragraph 2.8:-

2.9.1 on an annual basis by no later than each anniversary of the Commencement Date;

2.9.2 when there are any material changes to the security of the Services and/or associated processed and the Contractor System; and

2.9.3 within twenty (20) Business Days after a request from the DCC.

2.10 In relation to any updated version of the Security Management Plan under Paragraph 2.8, the Parties shall comply with the procedure set out in Paragraphs 2.3 to 2.7 (inclusive) relating to the approval by the DCC of the updated version of the Security Management Plan.

3. SECURITY COMPLIANCE

3.1 The DCC shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the Contractor maintains compliance with the Security Policy and the Security Management Plan, the specific security requirements set out in this Agreement and the Security Controls.

3.2 If, on the basis of evidence provided by such audits, it is the DCC's reasonable opinion that:-

3.2.1 the Contractor is not complying with any of the Security Policy, the Security Management Plan or the specific security requirements set out in this Agreement; and/or

3.2.2 the Security Controls are not being applied by the Contractor,

then the DCC shall notify the Contractor of the instance of non-compliance and give the Contractor reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement any necessary remedy.

4. SECURITY CONTROLS

4.1 The Contractor shall implement an information classification and handling scheme. This shall acknowledge that information originating from the DCC will be classified according to the DCC information scheme and will be suitably protected. Without prejudice to the provisions of Clause 35 (*DCC Data*) the Contractor shall:-

4.1.1 provide the DCC with all DCC Data on demand in an agreed open format;

4.1.2 have documented processes to guarantee availability of DCC Data in the event of the Contractor ceasing to trade;

4.1.3 develop, maintain, and hold all DCC Data in accordance with the DCC data retention policies or any other relevant instruction provided by the DCC;

4.1.4 securely destroy all media that has held DCC Data at the end of life of that media in line with Good Industry Practice so as to prevent the retrieval of the DCC Data ; and

4.1.5 securely erase any or all DCC Data when requested to do so by the DCC so as to prevent the later retrieval of the DCC Data.

4.2 Without prejudice to the provisions of Clause 30 (*Contractor Personnel*) the Contractor shall ensure that:-

4.2.1 all Contractor Personnel shall be subject to pre-employment checks that conform to Good Industry Practice and that include, as a minimum:-

(a) employment history for at least the last three years;

(b) proof of identity;

(c) checks to identify unspent criminal convictions; and

(d) confirmation of right to live and work in the UK (including nationality and immigration status).

4.2.2 all Contractor Personnel that have the ability to access DCC Data or Systems holding such data shall be informed of their responsibilities and undergo regular training on secure information management principles relevant to their role;

4.2.3 the training described in Paragraph 4.2.2 shall include Contractor controls relating to home and mobile working outside of Contractor premises, secure information transfer, and the use of removable devices. Unless otherwise agreed with DCC in writing, the Contractor shall ensure that this training is undertaken annually.

4.3 The Contractor shall ensure that at all times it is able to confirm to the DCC the Contractor physical locations in which DCC Data is or may be stored, processed and managed from, and the applicable legal and regulatory frameworks to which DCC Data is subject. Where third party hosting or services are used to process or store DCC Data, the Contractor shall be able to confirm to the DCC the third parties used.

4.4 The Contractor shall not store, process or administer DCC Data outside of the UK without the prior written consent of the DCC.

4.5 The Contractor shall ensure that Systems used to access or manage DCC Data shall be under the management authority and control of the Contractor and shall have a minimum set of security policy configuration enforced by the Contractor in accordance with Good Industry Practice.

4.6 The Contractor shall ensure that:-

4.6.1 the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice;

4.6.2 when DCC Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or service that is recognised as providing a standard that is consistent with Good Industry Practice;

4.6.3 the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) shall be applied to the design and configuration of the Contractor Solution.

4.7 The Contractor shall operate an access control regime to ensure all users and administrators of the Contractor System are uniquely identified and authenticated when accessing or administrating the Contractor System. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the Contractor System they require. The Contractor shall retain an audit record of accesses.

4.8 The Contractor shall notify the DCC as soon as reasonably practicable upon becoming aware of any security vulnerability in the Contractor Solution and/or any likely cause of any material adverse effect on any aspect of the Contractor Solution.

4.9 The Contractor shall procure the application of security patches to vulnerabilities within such time periods as defined in the Security Management Plan based on Good Industry Practice for categorising vulnerabilities, except where:-

4.9.1 the Contractor can demonstrate that a vulnerability is not exploitable within the context of the Contractor Solution; or

4.9.2 the application of a security patch adversely affects the Contractor's ability to deliver the Services in which case the Contractor shall request an extension from the DCC that includes a security patch test plan.

4.10 The Contractor shall ensure that the Contractor Solution is maintained with the provision for major version upgrades of all commercial off-the-shelf software to be upgraded within six (6) months of the release of the latest version, such that it is no more than one major version level below the latest release throughout the Term unless:-

4.10.1 where upgrading such commercial off-the-shelf software reduces the level of mitigations to known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within twelve (12) months of release of the latest version; or

4.10.2 agreed otherwise with the DCC in writing.

4.11 The Contractor shall ensure that commercial-off-the-shelf software used in the Contractor Solution is supported by the software supplier. Where support has lapsed or otherwise removed then the Contractor shall upgrade to a version that is supported or change the software used unless agreed otherwise with the DCC in writing.

4.12 The Contractor shall collect audit records which relate to security events in the Contractor System or that would support the analysis of potential or actual

compromises in or related to the Contractor System. In order to facilitate effective monitoring and forensic readiness the Contractor shall ensure that the audit records should as a minimum include:-

4.12.1 logs to facilitate the identification of the specific asset which makes every outbound request external to the IT environment (to the extent that the IT environment is within the control of the Contractor). Such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers;

4.12.2 security events generated in the IT environment (to the extent that the IT environment is within the control of the Contractor) and shall include: privileged account logon and logoff events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

4.13 The Contractor shall retain audit records collected in accordance with Paragraph 4.12 for a period of at least six (6) months.

4.14 The Contractor shall notify the DCC in accordance with the agreed security incident management process described in the Security Management Plan upon becoming aware of any Breach of Security, suspected Breach of Security or attempted Breach of Security.

4.15 Without prejudice to the security incident management process set out in the Security Management Plan, upon becoming aware of any Breach of Security, suspected Breach of Security or attempted Breach of Security the Contractor shall:-

4.15.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the DCC) necessary to:-

(a) minimise the extent of action or potential harm caused by the breach;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Services;

(c) apply a tested mitigation against any such Breach of Security; and

(d) prevent a further Breach of Security in the future exploiting the same root cause.

4.15.2 as soon as reasonably practicable provide to the DCC full details of the Breach of Security, suspected Breach of Security or attempted Breach of Security, including a root cause analysis where requested by the DCC.

4.16 In the event that any action is taken in response to a Breach of Security, suspected Breach of Security or attempted Breach of Security that demonstrates non-compliance with the Contractor's Security Policy and Security Management Plan, the specific security requirements set out in this

Agreement and/or the Security Controls, then any required changes and/or action shall be implemented at no cost to the DCC.

5. INDEPENDENCE OF SYSTEMS

5.1 The Contractor shall ensure that no Contractor Person is engaged in:-

5.1.1 the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of the DCC Live Systems; or

5.1.2 the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the DCC Live Systems, unless that individual satisfies the requirements of Paragraph 5.2.

5.2 A Contractor Person satisfies the requirements of this Paragraph 5.2 only if, at any time at which that individual is engaged in any activity described in Paragraph 5.1, he or she:-

5.2.1 is not at the same time also engaged in:-

(a) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any User Systems; or

(b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any User Systems; and

5.2.2 has not been engaged in any activity described in Paragraph 5.2.1 for a period of time which the DCC reasonably considers to be appropriate.