Order Schedule 9 (Security)

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("**ICT**"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or (b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the Security Policy where the Buyer has required compliance with;
"Certification Requirements"	means the information security requirements set out in Paragraph 6.1 and 6.2;
"CHECK Service Provider"	means a company which, under the CHECK Scheme: (a) has been certified by the NCSC; (b) holds "Green Light" status; and (c) is authorised to provide the IT Health Check services required by Paragraph 7;
"CREST Service Provider"	means a company with an information security accreditation of a security operations centre qualification from CREST International;
"Cyber Essentials"	means the Cyber Essentials scheme operated by the National Cyber Security Centre;
"IT Health Check"	means the security testing of the Supplier System;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, as updated from time to time.

2. Complying with security requirements and updates to them

2.1 The Buyer and the Supplier recognise that, where specified in DPS Schedule 4 (DPS Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or handle Government Data comply with the requirements of this Order Schedule 9.

2.3 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.4 Where the Security Policy applies, the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.5 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.6 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data;

3.2.4 where specified by the Buyer in accordance with Paragraph 2.3 complies with the Security Policy; and

3.2.5 complies with the 14 Cloud Security Principles available at: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles. The Supplier must document how it and any cloud service providers they use comply with these principles as part of the Security Management Plan, and provide this documentation upon request by the Buyer.

3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

4.1 **Introduction**

4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 **Content of the Security Management Plan**

4.2.1 The Security Management Plan shall:

(a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

(b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

(c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

(d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

(e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

(f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with the Security Policy as set out in Paragraph 2.3; and

(g) be written in plain English (as far as is practicable) in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 **Development of the Security Management Plan**

4.3.1 By the date in the Implementation Plan, and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However, a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.3 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 **Amendment of the Security Management Plan**

4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Deliverables and/or associated processes;

(c) where necessary in accordance with Paragraph 2.4, any change to the Security Policy;

(d) any new perceived or changed security threats; and

(e) any reasonable change in requirements requested by the Buyer.

4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

(a) suggested improvements to the effectiveness of the Security Management Plan;

(b) updates to the risk assessments; and

(c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the Supplier's security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

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

(a) minimise the extent of actual or potential harm caused by any Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

(c) prevent an equivalent breach in the future exploiting the same cause failure; and

(d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with Paragraph 2.3) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

6. Certification requirements

6.1 The Supplier shall be certified as compliant with, and shall ensure that each Key Subcontractor is certified as compliant with, either:

6.1.1 ISO/IEC 27001 (at least ISO/IEC 27001:2013) by a UK Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); or:

6.1.2 Cyber Essentials PLUS.

6.2 The Supplier shall ensure that each non-Key Subcontractor is certified as compliant with Cyber Essentials.

6.3 The Supplier shall provide the Buyer with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or process Buyer Data, and shall maintain such certificates of compliance throughout the Order Contract Period.

7. Testing

7.1 The Supplier must:

7.1.1 prior to the date in the Implementation Plan; and

7.1.2 at least once during each Contract Year following Achievement of the MVP Deployed Milestone;

undertake the following activities:

7.1.3 conduct security testing of the Supplier System (an **"IT Health Check"**);

7.1.4 implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Annex 1 Paragraph 11.

7.2 In arranging an IT Health Check, the Supplier must:

7.2.1 use only a CHECK Service Provider or CREST Service Provider to perform the IT Health Check;

7.2.2 design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier System and the delivery of the Services;

7.2.3 ensure that the scope of the IT Health Check encompasses the components of the Supplier System used to access, store, handle or manage Government Data; and

7.2.4 ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

Annex 1: Baseline security requirements

1. Handling Classified information

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre ("**NCSC**") to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("**CPA**").

2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

3.2 The Supplier shall not and shall procure that none of its Subcontractors process Buyer Data outside the UK and Ireland without the prior written consent of the Buyer, which may be subject to conditions.

3.3 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.4 The Supplier shall:

3.4.1 provide the Buyer with all Government Data on demand in an agreed open format;

3.4.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

3.4.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.4.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

3.5 The Supplier shall ensure that the Supplier and each Subcontractor who is responsible for the secure destruction of Buyer Data:

3.5.1 securely destroys Buyer Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013);

3.5.2 should satisfy the Buyer that their data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and

3.5.3 must maintain an asset register of all Buyer supplied information, data and equipment to ensure Buyer assets are returned and/or deleted.

3.6 The Supplier shall provide the Buyer with evidence of its and its Subcontractor's compliance with the requirements set out in this Paragraph 3 before the Supplier or the relevant Subcontractor (as applicable) may carry out the secure destruction of any Buyer Data.

4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that 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.

5. Security by design

5.1 The Supplier shall apply the "principle of least privilege" (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the Operating Environment (to the extent that the Operating Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the Operating Environment (to the extent that the Operating Environment is within the control of the Supplier).

6. Security of Supplier Staff

6.1 All Supplier Staff shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The Buyer may permit the Supplier to deviate from the pre-employment checks which are required by the HMG Baseline Personnel Security Standard for any Supplier Staff who are not based in the UK. Any permission must be in writing to be effective.

6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as "SC") including system administrators with privileged access to IT systems which store or process Government Data.

6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data, except where agreed with the Buyer in writing.

6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the Operating Environment (to the extent that the Operating Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the "principle of least privilege", users and administrators shall be allowed access only to those parts of the Operating Environment that they require. The Supplier shall retain an audit record of accesses.

8. Audit

8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

8.1.1 logs to facilitate the identification of the specific asset which makes every outbound request external to the Operating Environment (to the extent that the Operating Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 security events generated in the Operating Environment (to the extent that the Operating Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off 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.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the Operating Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least six (6) Months.

9. **Protective monitoring system**

9.1 The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reporting, analysing access to and use of the Supplier System and the Government Data to:

9.1.1 identify and prevent any potential Breach of Security;

9.1.2 respond effectively and in a timely manner to any Breach of Security that does occur;

9.1.3 identify and implement changes to the Supplier System to prevent future any Breach of Security; and

9.1.4 help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier System,

(together the **"Protective Monitoring System"**).

9.2 The Protective Monitoring System must provide for:

9.2.1 event logs and audit records of access to the Supplier System; and

9.2.2 regular reports and alerts to identify:

a) changing access trends;

b) unusual usage patterns; or

c) the access of greater than usual volumes of Government Data; and

9.2.3 the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

10. Vulnerability scanning

10.1 The Supplier must:

10.1.1 scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and

10.1.2 if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 11.

11. Patching

11.1 The Supplier must, and must ensure that Subcontractors, treat any public releases of patches for vulnerabilities as follows:

11.1.1 the Supplier must patch any vulnerabilities classified as "critical" within 5 Working Days of the public release, unless otherwise agreed with the Buyer in writing;

11.1.2 the Supplier must patch any vulnerabilities classified as "important" within 1 month of the public release, unless otherwise agreed with the Buyer in writing;

11.1.3 the Supplier must patch any vulnerabilities classified as "other" within 2 months of the public release, unless otherwise agreed with the Buyer in writing;

11.1.4 , where it is not technically feasible to patch the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability, which shall be agreed with the Buyer in writing.