S1 - PRECEDENT CONTRACT FOR THE PURCHASE OF SERVICES

SECTION A

This Contract is dated [ ] 2017.

Parties

(1) **Innovate UK,** Polaris House, North Star Avenue, Swindon SN2 1FL (**the Customer**)

(2) **[ ]**, [a company incorporated and registered in [COUNTRY] with company number [NUMBER] and registered VAT number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS]] [a partnership under the laws of [COUNTRY] whose address is [ADDRESS]] [a business with its trading address at [ADDRESS]] (**the Supplier**).

Background

The Customer wishes the Supplier to supply, and the Supplier wishes to supply, the Services defined below) in accordance with the terms of the Contract (as defined below).

A1 Interpretation

A1-1 **Definitions.** In the Contract (as defined below), the following definitions apply:

Business Day: a day (other than a Saturday, Sunday or public holiday) when banks in London are open for business.

Charges: the charges payable by the Customer for the supply of the Services in accordance with clause B4.

Conditions: the terms and conditions set out in this document as amended from time to time in accordance with clause C8-11.

Confidential Information: any confidential information, know how and data (in any form or medium) which relates to the Customer, UK SBS or the Supplier, including information relating to the businesses of the Customer or the Supplier and information relating to their staff, finances, policies and procedures. This includes information identified as confidential in the Order or the Special Conditions (if any).

Contract: the contract between the Customer and the Supplier for the supply of the Services, in accordance with these Conditions, any Special Conditions and the Order only.

Customer: the parties to the contract as named in Section A (1).

Deliverables: all Documents, products and materials developed by the Supplier or its agents, contractors and employees as part of or in relation to the Services in any form, including computer programs, data, reports and specifications (including drafts).

Document: includes, in addition to any document in writing, any drawing, map, plan, diagram, design, picture or other image, tape, disk or other device or record embodying information in any form.

EIR: the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant government department in relation to such regulations.

FOIA: the Freedom of Information Act 2000 and any subordinate legislation made under the Act from time to time, together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such legislation.

Information: has the meaning given under section 84 of FOIA.

Intellectual Property Rights: all patents, rights to inventions, utility models, copyright and related rights, trade marks, service marks, trade, business and domain names, rights in trade dress or get-up, rights in goodwill or to sue for passing off, unfair competition rights, rights in designs, rights in computer software, database right, topography rights, rights in confidential information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered and including all applications for and renewals or extensions of such rights, and all similar or equivalent rights or forms of protection in any part of the world.

Order: the Customer's order for the Services, as set out in the Customer's completed purchase order form (including any Specification) which is in the format of the pro forma order form attached at Schedule 2. For the avoidance of doubt, if the Customer's purchase order form is not in the format of the pro forma order form at Schedule 2, it will not constitute an Order.

Public Body: any part of the government of the United Kingdom including but not limited to the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales, local authorities, government ministers and government departments and government agencies.

UK SBS: UK Shared Business Services Ltd (formerly RCUK Shared Services Centre Ltd) (a limited company registered in England and Wales with company number 06330639).

Request for Information: a request for Information or an apparent request under FOIA or EIR.

Services: the services, including without limitation any Deliverables, to be provided by the Supplier under the Contract as set out in the Order.

Special Conditions: the special conditions (if any) set out in Schedule 1.

Specification: any specification for the Services, including any related plans and drawings, that is supplied to the Supplier by the Customer, or produced by the Supplier and agreed in writing by the Customer.

Supplier or Suppliers: the parties to the contract as named in Section A (2).

Supplier's Associate: any individual or entity associated with the Supplier including, without limitation, the Supplier's subsidiary, affiliated or holding companies and any employees, agents or contractors of the Supplier and / or its subsidiary, affiliated or holding companies or any entity that provides services for or on behalf of the Supplier.

TUPE: the Transfer of Undertakings (Protection of Employment) Regulations 2006 as amended or replaced from time to time.

Working Day: any Business Day excluding 27, 28, 29, 30 and 31 December in any year.

A1-2 **Construction.** In the Contract, unless the context requires otherwise, the following rules apply:

A1-2-1 A **person** includes a natural person, corporate or unincorporated body (whether or not having separate legal personality).

A1-2-2 A reference to a party includes its personal representatives, successors or permitted assigns.

A1-2-3 A reference to a statute or statutory provision is a reference to such statute or provision as amended or re-enacted. A reference to a statute or statutory provision includes any subordinate legislation made under that statute or statutory provision, as amended or re-enacted.

A1-2-4 Any phrase introduced by the terms **including**, **include**, **in particular** or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

A1-2-5 The headings in these Conditions are for ease of reference only and do not affect the interpretation or construction of the Contract.

A1-2-6 A reference to **writing** or **written** includes faxes and e-mails.

A2 Basis of contract

A2-1 Not Used.

A2-2 These Conditions, any Special Conditions and the Order apply to the Contract to the exclusion of all other terms and conditions, including any other terms that the Supplier seeks to impose or incorporate (whether in any quotation, confirmation of order, in correspondence or in any other context), or which are implied by trade, custom, practice or course of dealing.

A2-3 If there is any conflict or inconsistency between these Conditions, the Special Conditions (if any) and the Order (including any Specification), the Order (including any Specification) will prevail over the Special Conditions and the Special Conditions will prevail over these Conditions, in each case to the extent necessary to resolve that conflict or inconsistency.

A2-4 The Order constitutes an offer by the Customer to purchase the Services in accordance with these Conditions (and any Special Conditions). This offer shall remain valid for acceptance by the Supplier, in accordance with clause A2-5, for 28 days from the date of the Order. Notwithstanding that after 28 days the offer will have expired, the Customer may, at its discretion, nevertheless treat the offer as still valid and may elect to accept acceptance by the Supplier, in accordance with clause A2-5, as valid acceptance of the offer.

A2-5 Subject to clause A2-4, the Order shall be deemed to be accepted on the earlier of:

A2-5-1 the Supplier issuing a written acceptance of the Order; and

A2-5-2 the Supplier doing any act consistent with fulfilling the Order,

at which point the Contract shall come into existence. The Contract shall remain in force until all the parties' obligations have been performed in accordance with the Contract, at which point it shall expire, or until the Contract has been terminated in accordance with clause C2-3.

A3 Termination

A3-1 The Customer may terminate the Contract in whole or in part at any time before the Services are provided with immediate effect by giving the Supplier written notice, whereupon the Supplier shall discontinue all work on the Contract. The Customer shall pay the Supplier fair and reasonable compensation for work-in-progress at the time of termination, but such compensation shall not include loss of anticipated profits or any consequential loss. The Supplier shall have a duty to mitigate its costs and shall on request provide proof of expenditure for any compensation claimed.

A3-2 The Customer may terminate the Contract with immediate effect by giving written notice to the Supplier if:

A3-2-1 the circumstances set out in clauses B2-1-1 or C4-1 apply;

A3-2-2 the Supplier breaches any term of the Contract and (if such breach is remediable) fails to remedy that breach within 30 days of being notified in writing of the breach; or

A3-2-3 the Supplier suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or (being a company) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986, or (being an individual) is deemed either unable to pay its debts or as having no reasonable prospect of so doing, in either case, within the meaning of section 268 of the Insolvency Act 1986, or (being a partnership) has any partner to whom any of the foregoing apply; or

A3-2-4 the Supplier commences negotiations with all or any class of its creditors with a view to rescheduling any of its debts, or makes a proposal for or enters into any compromise or arrangement with its creditors; or

A3-2-5 (being a company) a petition is filed, a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of the Supplier; or

A3-2-6 (being an individual) the Supplier is the subject of a bankruptcy petition or order; or

A3-2-7 a creditor or encumbrancer of the Supplier attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of its assets and such attachment or process is not discharged within 14 days; or

A3-2-8 (being a company) an application is made to court, or an order is made, for the appointment of an administrator or if a notice of intention to appoint an administrator is given or if an administrator is appointed over the Supplier; or

A3-2-9 (being a company) a floating charge holder over the Supplier's assets has become entitled to appoint or has appointed an administrative receiver; or

A3-2-10 a person becomes entitled to appoint a receiver over the Supplier's assets or a receiver is appointed over the Supplier's assets; or

A3-2-11 any event occurs, or proceeding is taken, with respect to the Supplier in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned in clause A3-2-3 to clause A3-2-10 inclusive; or

A3-2-12 there is a change of control of the Supplier (within the meaning of section 1124 of the Corporation Tax Act 2010); or

A3-2-13 the Supplier suspends, or threatens to suspend, or ceases or threatens to cease to carry on, all or substantially the whole of its business; or

A3-2-14 the Supplier's financial position deteriorates to such an extent that in the Customer's opinion the Supplier's capability to adequately fulfil its obligations under the Contract has been placed in jeopardy; or

A3-2-15 (being an individual) the Supplier dies or, by reason of illness or incapacity (whether mental or physical), is incapable of managing his or her own affairs or becomes a patient under any mental health legislation.

A3-3 Termination of the Contract, however arising, shall not affect any of the parties' rights and remedies that have accrued as at termination. Clauses which expressly or by implication survive termination or expiry of the Contract shall continue in full force and effect.

A3-4 Without prejudice to clause A3-3, clauses B1, B2, B5, B6, B7, B8, B9, C1, C2-3, C7 and C8 shall survive the termination or expiry of the Contract and shall continue in full force and effect.

A3-5 Upon termination or expiry of the Contract, the Supplier shall immediately:

A3-5-1 cease all work on the Contract;

A3-5-2 deliver to the Customer all Deliverables and all work-in-progress whether or not then complete. If the Supplier fails to do so, then the Customer may enter the Supplier's premises and take possession of them. Until they have been returned or delivered, the Supplier shall be solely responsible for their safe keeping and will not use them for any purpose not connected with this Contract;

A3-5-3 cease use of and return (or, at the Customer's election, destroy) all Customer Materials in the Supplier's possession or control; and

A3-5-4 cease all use of, and delete all copies of, the Customer's confidential information.

A3-7 The Customer shall at any time have the right for convenience to terminate the Contract or reduce the quantity of Services or Goods to be provided by the Supplier in each case by giving to the Supplier reasonable written notice. During the period of notice the Customer may direct the Supplier to perform all or any of the work under the Contract. Where the Customer has invoked either of these rights, the Supplier may claim reasonable costs necessarily and properly incurred by him as a result of the termination or reduction, excluding loss of profit, provided that the claim shall not exceed the total cost of the Contract.

SECTION B

B1 Supply of Services

B1-1 The Supplier shall from the date set out in the Order and until the end date specified in the Order provide the Services to the Customer in accordance with the terms of the Contract.

B1-2 The Supplier shall meet any performance dates for the Services (including the delivery of Deliverables) specified in the Order or notified to the Supplier by the Customer.

B1-3 In providing the Services, the Supplier shall:

B1-3-1 co-operate with the Customer in all matters relating to the Services, and comply with all instructions of the Customer;

B1-3-2 perform the Services with the best care, skill and diligence in accordance with best practice in the Supplier's industry, profession or trade

B1-3-3 use personnel who are suitably skilled and experienced to perform tasks assigned to them, and in sufficient number to ensure that the Supplier's obligations are fulfilled in accordance with this Contract;

B1-3-4 ensure that the Services and Deliverables will conform with all descriptions and specifications set out in the Order, and that the Deliverables shall be fit for any purpose expressly or impliedly made known to the Supplier by the

Customer;

B1-3-5 provide all equipment, tools and vehicles and such other items as are required to provide the Services;

B1-3-6 use the best quality goods, materials, standards and techniques, and ensure that the Deliverables, and all goods and materials supplied and used in the Services or transferred to the Customer, will be free from defects in workmanship, installation and design;

B1-3-7 obtain and at all times maintain all necessary licences and consents, and comply with all applicable laws and regulations;

B1-3-8 observe all health and safety rules and regulations and any other security requirements that apply at any of the Customer's premises; and

B1-3-9 not do or omit to do anything which may cause the Customer to lose any licence, authority, consent or permission on which it relies for the purposes of conducting its business, and the Supplier acknowledges that the Customer may rely or act on the Services.

B1-4 The Customer's rights under the Contract are without prejudice to and in addition to the statutory terms implied in favour of the Customer under the Supply of Goods and Services Act 1982 and any other applicable legislation.

B1-5 Without prejudice to the Customer's statutory rights, the Customer will not be deemed to have accepted any Deliverables until the Customer has had at least 14 Working Days after delivery to inspect them and the Customer also has the right to reject any Deliverables as though they had not been accepted for 14 Working Days after any latent defect in the Deliverables has become apparent.

B1-6 If, in connection with the supply of the Services, the Customer permits any employees or representatives of the Supplier to have access to any of the Customer's premises, the Supplier will ensure that, whilst on the Customer's premises, the Supplier's employees and representatives comply with:

B1-6-1 all applicable health and safety, security, environmental and other legislation which may be in force from time to time; and

B1-6-2 any Customer policy, regulation, code of practice or instruction relating to health and safety, security, the environment or access to and use of any Customer laboratory, facility or equipment which is brought to their attention or given to them whilst they are on Customer premises by any employee or representative of the Customer.

B1-7 The Supplier warrants that the provision of Services shall not give rise to a transfer of any employees of the Supplier or any third party to the Customer pursuant to

TUPE.

B2 Customer remedies

B2-1 If the Supplier fails to perform the Services by the applicable dates, the Customer shall, without limiting its other rights or remedies, have one or more of the following rights:

B2-1-1 to terminate the Contract with immediate effect by giving written notice to the Supplier;

B2-1-2 to refuse to accept any subsequent performance of the Services (including delivery of Deliverables) which the Supplier attempts to make;

B2-1-3 to recover from the Supplier any costs incurred by the Customer in obtaining substitute services from a third party;

B2-1-4 where the Customer has paid in advance for Services that have not been provided by the Supplier, to have such sums refunded by the Supplier; or

B2-1-5 to claim damages for any additional costs, loss or expenses incurred by the Customer which are in any way attributable to the Supplier's failure to meet such dates.

B2-2 These Conditions shall extend to any substituted or remedial services provided by the Supplier.

B2-3 The Customer's rights under this Contract are in addition to its rights and remedies implied by statute and common law.

B3 Customer's obligations

B3-1 The Customer shall:

B3-1-1 provide the Supplier with reasonable access at reasonable times to the Customer's premises for the purpose of providing the Services; and

B3-1-2 provide such information to the Supplier as the Supplier may reasonably request and the Customer considers reasonably necessary for the purpose of providing the Services.

B4 Charges and payment

B4-1 The Charges for the Services shall be set out in the Order, and shall be the full and exclusive remuneration of the Supplier in respect of the performance of the Services. Unless otherwise agreed in writing by the Customer, the Charges shall include every cost and expense of the Supplier directly or indirectly incurred in connection with the performance of the Services.

B4-2 Where the Order states that the Services are to be provided on a time and materials basis, the Charges for those Services will be calculated as follows:

B4-2-1 the charges payable for the Services will be calculated in accordance with the Supplier's standard daily fee rates (as at the date of the Order), subject to any discount specified in the Order;

B4-2-2 the Supplier's standard daily fee rates for each individual person will be calculated on the basis of an eight-hour day worked between such hours and on such days as are agreed by the Customer and the Supplier;

B4-2-3 the Supplier will not be entitled to charge pro-rata for part days without the prior written consent of the Customer;

B4-2-4 the Supplier will ensure that every individual whom it engages to perform the Services completes time sheets recording time spent on the Services and the Supplier will use such time sheets to calculate the charges covered by each invoice and will provide copies of such time sheets to the Customer upon request; and

B4-2-5 the Supplier will invoice the Customer monthly in arrears for its charges for time, as well as any previously agreed expenses and materials for the month concerned calculated as provided in this clause B4-2 and clause B4-3

B4-3 The Customer will reimburse the Supplier at cost for all reasonable travel, subsistence and other expenses incurred by individuals engaged by the Supplier in providing the Services to the Customer provided that the Customer's prior written approval is obtained before incurring any such expenses, that all invoices for such expenses are accompanied by valid receipts and provided that the Supplier complies at all times with the Customer’s expenses policy from time to time in force.

B4-4 The Supplier shall invoice the Customer on completion of the Services. Each invoice shall include such supporting information required by the Customer to verify the accuracy of the invoice, including but not limited to the relevant purchase order number.

B4-5 In consideration of the supply of the Services by the Supplier, the Customer shall pay the invoiced amounts within 30 days of the date of a correctly rendered invoice. Payment shall be made to the bank account nominated in writing by the Supplier unless the Customer agrees in writing to another payment method.

B4-6 All amounts payable by the Customer under the Contract are exclusive of amounts in respect of value added tax chargeable for the time being (**VAT**). Where any taxable supply for VAT purposes is made under the Contract by the Supplier to the Customer, the Customer shall, on receipt of a valid VAT invoice from the Supplier, pay to the Supplier such additional amounts in respect of VAT as are chargeable on the supply of the Services at the same time as payment is due for the supply of the Services.

B4-7 The Supplier shall maintain complete and accurate records of the time spent and materials used by the Supplier in providing the Services, and shall allow the Customer to inspect such records at all reasonable times on request.

B4-8 The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Customer in order to justify withholding payment of any such amount in whole or in part. The Customer may, without limiting any other rights or remedies it may have, set off any amount owed to it by the Supplier against any amounts payable by it to the Supplier under the Contract.

B4-9 The Supplier acknowledges and agrees that it will pay correctly rendered invoices from any of its suppliers or other sub-contractors within 30 days of receipt of the invoice.

B5 Customer property

B5-1 The Supplier acknowledges that all information (including confidential information), equipment and tools, drawings, specifications, data, software and any other materials supplied by UK SBSand the Customer to the Supplier (**Customer Materials**) and all rights in the Customer Materials are and shall remain at all times the exclusive property of the Customer. The Supplier shall keep the Customer Materials in safe custody at its own risk, maintain them in good condition until returned to the Customer, and not dispose or use the same other than for the sole purpose of performing the Supplier's obligations under the Contract and in accordance with the Customer's written instructions or authorisation.

B6 Intellectual property rights

B6-1 In respect of any goods that are transferred to the Customer under this Contract, including without limitation the Deliverables or any part of them, the Supplier warrants that it has full clear and unencumbered title to all such items, and that at the date of delivery of such items to the Customer, it will have full and unrestricted rights to transfer all such items to the Customer.

B6-2 Save as otherwise provided in the Special Conditions, the Supplier assigns to the Customer, with full title guarantee and free from all third party rights, all Intellectual Property Rights in the products of the Services, including for the avoidance of doubt the Deliverables. Where those products or Deliverables incorporate any Intellectual Property Rights owned by or licensed to the Supplier which are not assigned under this clause, the Supplier grants to the Customer a worldwide, irrevocable, royalty-

free, transferable licence, with the right to grant sub-licences, under those Intellectual Property Rights to maintain, repair, adapt, copy and use those products and Deliverables for any purpose.

B6-3 The Supplier shall obtain waivers of all moral rights in the products, including for the avoidance of doubt the Deliverables, of the Services to which any individual is now or may be at any future time entitled under Chapter IV of Part I of the Copyright Designs and Patents Act 1988 or any similar provisions of law in any jurisdiction.

B6-4 The Supplier shall, promptly at UK SBSor the Customer's request, do (or procure to be done) all such further acts and things and the execution of all such other documents as the Customer may from time to time require for the purpose of securing for the Customer the full benefit of the Contract, including all right, title and interest in and to the Intellectual Property Rights assigned to the Customer in accordance with clause B6-2.

B7 Indemnity

B7-1 The Supplier shall indemnify, and shall keep indemnified, the Customer in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, fines, legal and other professional fees and expenses awarded against or incurred or paid by the Customer as a result of or in connection with:

B7-1-1 any claim made against the Customer by a third party arising out of, or in connection with, the supply of the Services, to the extent that such claim arises out of the breach, negligent performance or failure or delay in performance of the Contract by the Supplier, its employees, agents or subcontractors; and

B7-1-2 any claim brought against the Customer for actual or alleged infringement of a third party's Intellectual Property Rights arising out of, or in connection with, the receipt, use or supply of the Services; and

B7-1-3 any claim whether in tort, contract, statutory or otherwise, demands, actions, proceedings and any awards arising from a breach by the Supplier of clause B1-7 of these Conditions.

B7-2 This clause B7 shall survive termination or expiry of the Contract.

B8 Insurance

B8-1 During the term of the Contract and for a period of 3 years thereafter, the Supplier shall maintain in force, with a reputable insurance company, professional indemnity insurance, employer liability insurance, product liability and public liability insurance to cover such heads of liability as may arise under or in connection with the Contract, and shall, on UK SBSor the Customer's request, produce both the insurance certificate giving details of cover and the receipt for the current year's

premium in respect of each insurance.

B9 Liability

B9-1 In this clause B9, a reference to the Customer's liability for something is a reference to any liability whatsoever which the Customer might have for it, its consequences, and any direct, indirect or consequential loss, damage, costs or expenses resulting from it or its consequences, whether the liability arises under the Contract, in tort or otherwise, and even if it results from the Customer's negligence or from negligence for which the Customer would otherwise be liable.

B9-2 the Customer is not in breach of the Contract, and the Customer shall not have any liability for anything, to the extent that the apparent breach or liability is attributable to the Supplier's breach of the Contract.

B9-3 Subject to clause B9-6, the Customer shall not have any liability for:

B9-3-1 any indirect or consequential loss or damage;

B9-3-2 any loss of business, rent, profit or anticipated savings;

B9-3-3 any damage to goodwill or reputation;

B9-3-4 loss, theft, damage or destruction to any equipment, tools, machinery, vehicles or other equipment brought onto the Customer's premises by or on behalf of the Supplier; or

B9-3-5 any loss, damage, costs or expenses suffered or incurred by any third party.

B9-4 Subject to clause B9-6, the Customer's total liability shall be limited to the Charges.

B9-5 Subject to clause B9-6, the Supplier's total liability in connection with the Contract shall be limited to £250,000

B9-6 Nothing in the Contract restricts either the Customer's or the Supplier's liability for:

B9-6-1 death or personal injury resulting from its negligence; or

B9-6-2 its fraud (including fraudulent misrepresentation); or

B9-6-3 breach of any obligations as to title implied by Section 12 of the Sale of Goods Act 1979 or Section 2 of the Supply of Goods and Services Act 1982.

SECTION C

C1 Confidential information

C1-1 A party (**Receiving Party**) shall keep in strict confidence all Confidential Information which has been disclosed to, or otherwise obtained by, the Receiving Party by the other party (**Disclosing Party**), its employees, agents or subcontractors. The Receiving Party shall restrict disclosure of such Confidential Information to such of its employees, agents or subcontractors as need to know it for the purpose of discharging the Receiving Party's obligations under the Contract, and shall ensure that such employees, agents or subcontractors are subject to obligations of confidentiality corresponding to those which bind the Receiving Party. This clause C1 shall survive termination or expiry of the Contract

C2 Transparency

C2-1 The Supplier acknowledges that the United Kingdom Government's transparency agenda requires that contracts, such as the Contract, and any sourcing document, such as the invitation to sourcing, are published on a designated, publicly searchable website.

C2-2 The Supplier acknowledges that, except for any information which is exempt from disclosure in accordance with the provisions of FOIA, the content of the Contract is not Confidential Information. UK SBS and the Customer shall be responsible for determining in their absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of FOIA.

C2-3 Notwithstanding any other term of the Contract, the Supplier hereby consents to the Customer and / or UK SBS publishing the Contract in its entirety, (but with any information which is exempt from disclosure in accordance with the provisions of FOIA redacted) including from time to time agreed changes to the Contract, to the general public.

C3 Force majeure

C3-1 If any event or circumstance that is beyond the reasonable control of the Supplier, and which by its nature could not have been foreseen by the Supplier or, if it could have been foreseen, was unavoidable, (provided that the Supplier shall use all reasonable endeavours to cure any such events or circumstances and resume performance under the Contract) prevent the Supplier from carrying out its obligations under the Contract for a continuous period of more than 10 Business Days, the Customer may terminate this Contract immediately by giving written notice to the Supplier

C4 Corruption

C4-1 The Customer shall be entitled to terminate the Contract immediately and to recover from the Supplier the amount of any loss resulting from such termination if the Supplier or a Supplier's Associate:

C4-1-1 offers or agrees to give any person working for or engaged by UK SBSthe Customer or any Public Body any favour, gift or other consideration, which could act as an inducement or a reward for any act or failure to act connected to the Contract, or any other agreement between the Supplier and the Customer or any Public Body, including its award to the Supplier or a Supplier's Associate and any of the rights and obligations contained within it;

C4-1-2 has entered into the Contract if it has knowledge that, in connection with it, any money has been, or will be, paid to any person working for or engaged by UK SBS, the Customer or any Public Body by or for the Supplier, or that an agreement has been reached to that effect, unless details of any such arrangement have been disclosed in writing to the Customer before the Contract is entered into;

C4-1-3 breaches the provisions of the Prevention of Corruption Acts 1889 to 1916, or the Bribery Act 2010; or

C4-1-4 gives any fee or reward the receipt of which is an offence under Section 117(2) of the Local Government Act 1972.

C4-2 For the purposes of clause C4-1, "loss" shall include, but shall not be limited to:

C4-2-1 The Customer's costs in finding a replacement supplier;

C4-2-2 direct, indirect and consequential losses; and

C4-2-3 any loss suffered by the Customer as a result of a delay in its receipt of the Goods.

C5 Data protection

C5-1 The Supplier shall comply at all times with all data protection legislation applicable in the UK from time to time.

Cyber essentials questionnaire

C5-2 The Supplier agrees that during any term or extension at the sole discretion of the Customer to complete the questionnaire provided in Schedule 3 as many times as is required within (14 days) from notice to do so and shall send this information as directed by the Customer. The Customer is required to provide such assurances to comply with government legislation. Any financial burden associated with the completion and submission of this questionnaire incurred by the Supplier shall not be reimbursable.

C6 Data protection

C6-1 The Supplier shall comply at all times with all data protection legislation applicable in the UK from time to time.

Cyber essentials questionnaire

CThe Supplier agrees that during any term or extension at the sole discretion of UK SBS or the Customer to complete the questionnaire provided in Annex A as many times as is required within (14 days) from notice to do so and shall send this information as directed by UK SBS or the Customer. UK SBS or the Customer is required to provide such assurances to comply with government legislation. Any financial burden associated with the completion and submission of this questionnaire incurred by the Supplier shall not be reimbursable.

C7 Freedom of information

C7-1 The Supplier acknowledges that UK SBS and the Customer may be subject to the requirements of FOIA and EIR and shall assist and co-operate with UK SBS or the Customer to enable them to comply with its obligations under FOIA and EIR.

C7-2 The Supplier shall and shall procure that its employees, agents, sub-contractors and any other representatives shall provide all necessary assistance as reasonably requested by UK SBS or the Customer to enable UK SBS or the Customer to respond to a Request for Information within the time for compliance set out in section 10 of FOIA or regulation 5 of EIR.

C7-3 UK SBS or the Customer shall be responsible for determining (in its absolute discretion) whether any Information:

C7-3-1 is exempt from disclosure in accordance with the provisions of FOIA or EIR;

C7-3-2 is to be disclosed in response to a Request for Information,

and in no event shall the Supplier respond directly to a Request for Information unless expressly authorised to do so in writing by UK SBS or the Customer.

C7-4 The Supplier acknowledges that UK SBS or the Customer may be obliged under the FOIA or EIR to disclose Information, in some cases even where that Information is commercially sensitive:

C7-4-1 without consulting with the Supplier, or

C7-4-2 following consultation with the Supplier and having taken its views into account.

C7-5 Where clause C7-4-2 applies UK SBS or the Customer shall, in accordance with any recommendations issued under any code of practice issued under section 45 of FOIA, take reasonable steps, where appropriate, to give the Supplier advanced notice, or failing that, to draw the disclosure to the Supplier's attention as soon as practicable after any such disclosure.

C7-6 Where the Supplier organisation is subject to the requirements of the FOIA and EIR, C6-7 will supersede C6-2 – C6-5. Where the Supplier organisation is not subject to the requirements of the FOIA and EIR, C6-7 will not apply.

C7-7 UK SBS and the Customer acknowledge that the Supplier may be subject to the requirements of the FOIA and EIR and shall assist and co-operate with the Supplier to enable them to comply with its obligations under the FOIA and EIR.

C8 General

C8-1 **Entire agreement.**

C8-1-1 The Contract constitutes the entire agreement between the Customer and the Supplier in relation to the supply of the Services and the Contract supersedes any earlier agreements, arrangements and understandings

relating to that subject matter.

C8-2 **Liability.**

C8-2-1 Where the Customer is more than one person, the liability of each such person for their respective obligations and liabilities under the Contract shall be several and shall extend only to any loss or damage arising out of each such person's own breaches.

C8-2-2 Where the Customer is more than one person and more than one of such persons is liable for the same obligation or liability, liability for the total sum recoverable will be attributed to the relevant persons in proportion to the price payable by each of them under the Contract.

C8-3 **Assignment and subcontracting.**

C8-3-1 The Customer may at any time assign, transfer, charge, subcontract or deal in any other manner with any or all of its rights or obligations under the Contract.

C8-3-2 The Supplier may not assign, transfer, charge, subcontract or deal in any other manner with any or all of its rights or obligations under the Contract without the Customer's prior written consent.

C8-3-3 Sub-Contractors

The Customer may (without cost to or liability of the Customer) require the Supplier to replace any subcontract or where in the reasonable opinion of the Customer any mandatory or discretionary grounds for exclusion referred to in Regulation 57 of the Public Contracts Regulations 2015 apply to the subcontractors.

C8-4 **Further assurance.**

C8-4-1 The Supplier will promptly at the Customer's request do (or procure to be done) all such further acts and things, including the execution of all such other documents, as the Customer may from time to time require for the purpose of securing for the Customer the full benefit of the Contract, including ensuring that all title in the Goods is transferred absolutely to the Customer.

C8-5 **Publicity**

C8-5-1 The Supplier shall not make any press announcements or publicise this Contract in any way without the Customer's prior written consent.

C8-5-2 UK SBS or the Customer shall be entitled to publicise this Contract in accordance with any legal obligation upon UK SBS or the Customer, including any examination of this Contract by the National Audit Office pursuant to the National Audit Act 1983 or otherwise.

C8-5-3 The Supplier shall not do anything or cause anything to be done, which may damage the reputation of UK SBSor the Customer or bring UK SBS or the Customer into disrepute.

C8-6 **Notices.**

C8-6-1 Any notice or other communication given to a party under or in connection with the Contract shall be in writing, addressed to:

C8-6-1-a in the case of the Customer:***Innovate UK***; Address: ***Polaris House, North Star Avenue, Swindon, Wiltshire SN2 1UE***; Email: ***Patrick.jarvis@innovateuk.gov.uk*** (and a copy of such notice or communication shall be sent to: Chief Procurement Officer, Polaris House, North Star Avenue, Swindon, Wiltshire SN2 1FF);

C8-6-1-b in the case of the Supplier: the address and email address set out in the Order,

or any other addressor email address which that party may have specified to the other party in writing in accordance with this clause C8-6, and shall be delivered personally, or sent by pre-paid first-class post, recorded delivery, commercial courier or e-mail.

C8-6-2 A notice or other communication shall be deemed to have been received: if delivered personally, when left at the address referred to in clause C-7-6-1; if sent by pre-paid first-class post or recorded delivery, at 9.00 am on the second Working Day after posting; if delivered by commercial courier, on the date and at the time that the courier's delivery receipt is signed; or, e-mail between the hours of 9.00am and 5.00pm on a Working Day, upon successful transmission ,or if sent by e-mail outside the hours of 9.00am and 5.00pm on a Working Day, at 9.00am on the next Working Day following successful transmission .

C8-6-3 Not Used.

C8-6-4 [Except for clause C8-6-5, t] [T]he provisions of this clause C8-6 shall not apply to the service of any proceedings or other documents in any legal action.

C8-6-5 [The Supplier irrevocably appoints and authorises [NAME] of [ADDRESS] (or such other person, being a firm of [solicitors] resident in England, as the Supplier may by notice substitute) to accept service on behalf of the Supplier of all legal process, and service on [NAME] (or any such substitute) shall be deemed to be service on the Supplier.]

C8-7 **Severance**

C8-7-1 If any court or competent authority finds that any provision of the Contract (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of the Contract shall not be affected.

C8-7-2 If any invalid, unenforceable or illegal provision of the Contract would be valid, enforceable and legal if some part of it were deleted, the provision shall apply with the minimum modification necessary to make it legal, valid and enforceable.

C8-8 **Waiver**. A waiver of any right or remedy under the Contract is only effective if given in writing and shall not be deemed a waiver of any subsequent breach or default. No failure or delay by a party to exercise any right or remedy provided under the Contract or by law shall constitute a waiver of that or any other right or remedy, nor shall it preclude or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall preclude or restrict the further exercise of that or any other right or remedy.

C8-9 No partnership, employment or agency. Nothing in the Contract creates any partnership or joint venture, nor any relationship of employment, between the Supplier and the Customer. Nothing in the Contract creates any agency between the Supplier and the Customer.

C8-10 **Third party rights**. A person who is not a party to this Contract shall not have any rights under or in connection with it, except that any member of the Associated Bodies or Authorised Entities that derives benefit under this Contract may directly enforce or rely on any terms of this Contract.

C8-11 **Variation**. Any variation to the Contract, including any changes to the Services, these Conditions, the Special Conditions or the Order, including the introduction of any additional terms and conditions, shall only be binding when agreed in writing by or on behalf of the Customer and the Supplier.

C8-12 **Governing law and jurisdiction.**

C8-12-1 Subject to clause C8-12-2, the Contract, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims), shall be governed by, and construed in accordance with, English law, and the parties irrevocably submit to the

exclusive jurisdiction of the courts of England and Wales.

C8-12-2 The Customer shall be free to enforce its intellectual property rights in any jurisdiction.

C8-13 **Modern Slavery Act 2015**

C8-13-1 During the Term or any extension of the Contract, the Customer is committed to ensuring that its supply chain complies with the above Act. The Supplier shall provide such assurances, on the anniversary of the commencement date or completion of the Contract, if less than 12 months.

C7-13-2 The Supplier shall provide a report covering the following but not limited to areas as relevant and proportionate to the Contract evidencing the actions taken, relevant to the Supplier and their supply chain associated with the Contract.

C7-13-2-1 Impact assessments undertaken

C7-13-2-2 Steps taken to address risk/actual instances of modern slavery and how actions have been prioritised

C7-13-2-3 Evidence of stakeholder engagement

C7-13-2-4 Evidence of ongoing awareness training

C7-13-2-5 Business-level grievance mechanisms in place to address modern slavery

C7-13-2-6 Actions taken to embed respect for human rights and zero tolerance of modern slavery throughout the organisation

C7-13-3 The Customer reserves the sole right to audit any and all reports submitted by the Supplier to an extent as deemed necessary and the Supplier shall unreservedly assist the Customer in doing so. Any financial burden incurred by the Supplier in doing so shall not be reimbursable.

C7-14 **Changes in costs resulting from changes to Government Legislation, Levies or Statutory Payments**

The Customer will reimburse during any term or extension (or, where such costs, awards or damages arise following termination/expiry) of this Agreement, any increases in the Supplier's cost of providing the Goods by reason of any modification or alteration to the Government legislation duties or levies or other statutory payments (including but not limited to National Insurance and/or VAT and/or introduction of or amendment to working time minimum wages). Subject always to open book access to the Supplier's records and always after a period of due diligence carried out by the Customer, relevant and proportionate to the value concerned.

C7-15 **Taxation obligations of the Supplier**

C7-15-1 The relationship between the Customer and the Supplier will be that of

"independent contractor" which means that the Supplier is not a employee, worker, agent or partner of the Customer and the Supplier will not give the impression that they are.

C7-15-2 As this is not an employment Contract the Supplier will be fully responsible for all their own tax including any national insurance contributions arising from carrying out the Services. If the Customer has to pay any such tax then the Supplier will pay back to Customer in full, any money that the Customer has to pay, and they will also pay back the Customer for any fine or other punishment imposed on the Customer because the tax or national insurance was not paid by the Supplier.

Schedule 1 Special Conditions

Schedule 2 Pro forma purchase order form

Schedule 3 Cyber Essentials Questionnaire

Schedule 3 - Cyber Essentials Questionnaire

Supplier Assurance Framework

Organisation:		**Contract Name;**		**Enquiry Type:**	RFI
Department:		**Date Completed:**			
Name:		**Position:**		**Contact Telephone Number:**	

Questionnaire			Information and Guidance			
Question	**Response**	**Response Comments**	**Question Guidance -** These are examples of the types of controls which maybe appropriate to manage the risks. However this list is not exhaustive. The importance thing here is to ensure the risks are identified and managed at a level which is acceptable to the delivery of the service and aligned to HMG departments risk appetite.	**Corresponding Framework**	**Risk Score/Indicator**	**Critical**
1.0 Introductory Questions						
1.1 To what part of your organisation does this self-assessment relate?	Please Select Answer					
1.2 Which of the following most closely describes the service you provide to us?						
Professional Services	Please Select Answer					
Information and Communications Technology (ICT) Services	Please Select Answer					
Business Process Outsourcing	Please Select Answer					
Estates, Facilities Management (FM), Guarding and Support Services	Please Select Answer					
Transport/Mail	Please Select Answer					
Storage/Archive	Please Select Answer					
Operational Equipment and Office Supplies	Please Select Answer					
Other	Please Select Answer					
1.3 Please provide more detail about your organisation/the service/the contract:	[Mandatory free text]					
1.4 Who is responsible for the security aspects of the service you provide? (Please Specify Full Name and Role)	[Mandatory free text]					
2.0 Risk Analysis - Risk can be defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to individuals and the organisation. The following section aims to help us determine which aspects of the service you provide increase the impact or likelihood of a compromise to the confidentiality, integrity or availability of our assets. The responses you provide here will determine the route you will take though the remainder of the self-assessment.						
2.1 Do you have access to, process or store any of **our assets** (including data) in the delivery of your service?	Please Select Answer		An asset could be information, personnel or any object with value (eg, a computer system, money, a passport etc). The Cabinet Office Security Policy Framework, and associated policy and guidance outlines the mandatory steps Government must take to protect our assets. Including those that are shared with suppliers and delivery partners.		If the supplier does not handle any Departmental assets then consideration should be given as to whether or not they should be in scope of the assessment. Exit self-assessment.	
2.2 Do you have access to, process or store **our data** in the delivery of your service?	Please Select Answer		Information is a key asset to Government and its correct handling is vital to the safe and effective delivery of public services. Some of the assessment focuses specifically on information assets. Your response to this question will impact on your route through the assessment.		Risk if the supplier Handles our Data. If the supplier does not handle any of our data then further investigation of the type of data they handle (sensitivity, number of records, where the data is held, type of access) is irrelevant. Skip: 2.3 - 2.11	
2.3 In the delivery of your service which of the following types of our data do you store/process?			If you are unsure of the classification of the assets that you process or store on our behalf you should consult your departmental contact before proceeding. The Information Commissioner's Office publish an official definition of personal and sensitive personal data. Found here: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx			
Personal data as defined by the Data Protection Act	Please Select Answer					
Sensitive personal as defined as the Data Protection Act	Please Select Answer					
OFFICIAL	Please Select Answer					
SECRET	Please Select Answer					
TOP SECRET	Please Select Answer					

Questionnaire			Information and Guidance			
Question	**Response**	**Response Comments**	**Question Guidance -** These are examples of the types of controls which maybe appropriate to manage the risks. However this list is not exhaustive. The importance thing here is to ensure the risks are identified and managed at a level which is acceptable to the delivery of the service and aligned to HMG departments risk appetite.	**Corresponding Framework**	**Risk Score/Indicator**	**Critical**
2.4 What volume of personal data do you process?	Please Select Answer				Above 1000 records	
2.5 Where is our data held?	Please Select Answer				Data Held Offshore	
2.6 Where is our data accessed from?	Please Select Answer				Data Accessed Offshore	
2.7 Which of the following describe the type of access you have to our data?	Please Select Answer				Ability to Amend our data	
2.8 Approximately how many of your staff have access to our assets?	Please Select Answer				Large numbers of staff access our data	
2.9 Do you use sub-contractors in the delivery of your service?	Please Select Answer				Use of Sub-contractors If the supplier does not use sub contractors in the delivery of their service then further probing with regards to the number of sub-contractors, or their compliance with our Security Policy, is unnecessary.	
2.10 How many of your subcontractors have access to our assets?	Please Select Answer				Sub-contractors have access to our assets	
2.11 Which of the following best describes how you use ICT systems to deliver your service?	Please Select Answer				Uses own systems, uses shared systems If the supplier uses Departmental ICT, or does not use ICT systems in the delivery of their service, then section 2 may not be relevant. Skip section 2	
2.12 In relation to the ICT systems used to deliver your service, which of the following is true?						
We permit the use of removable media	Please Select Answer				Allows use of removable media	
We permit remote working	Please Select Answer				Allows Remote working	
We allow staff to connect their own devices to our ICT systems	Please Select Answer				Allows BYOD	
2.13 Which of the following best describes the location from which you deliver your service?	Please Select Answer				If the supplier delivers from Departmental premises then section 2 may not be relevant. Skip section 2.	
2.14 Does any part of the service you deliver form part of the country's Critical National Infrastructure?	Please Select Answer				Part of CNI	
3.0 Information Systems - This section seeks to determine your approach to securing ICT systems used in the delivery of your service, in particular those that are used to process our information assets.						
3.1 Does your organisation hold any accreditations or certifications relating to ICT systems used in the delivery of your service?			All HMG activities attract risk. Risks need to be assessed by government organisations so that they can make informed, practical and effective business enabling decisions. Government organisations will have: A clearly-communicated set of security policies and procedures, which reflect business objectives to support good risk management;	SPF - Risk Management		
a) Yes, ICT system/s have been formally accredited by a government Department/Agency [Please provide details]	Please Select Answer				5	
b) Yes, ICT system/s are ISO27001:2013/2005 certified [Insert certificate number]	Please Select Answer				5	
c) Yes, ICT system/s are compliant with ISO27001:2013/2005	Please Select Answer				3	
d) Yes, our system/s are compliant with a standard that is aligned to ISO27001:2013/2005 [Please provide details]	Please Select Answer				3	
e) Yes, Cyber Essentials Plus [Insert certificate number]	Please Select Answer				0	

Questionnaire			Information and Guidance			
Question	**Response**	**Response Comments**	**Question Guidance -** These are examples of the types of controls which maybe appropriate to manage the risks. However this list is not exhaustive. The importance thing here is to ensure the risks are identified and managed at a level which is acceptable to the delivery of the service and aligned to HMG departments risk appetite.	**Corresponding Framework**	**Risk Score/Indicator**	**Critical**
f) Yes, Cyber Essentials	Please Select Answer					
3.2 Has a technical risk assessment been performed to identify a set of proportionate risk treatment controls?	Please Select Answer		a. A mature understanding of the security risks throughout the organisation, where appropriate this will be informed by the National Technical Authorities;	SPF - Risk Management	5 - Yes with review 3 - Yes 0 - No	Critical
3.3 Are security operating procedures in place governing the use of your ICT systems? Do these cover home and mobile working?	Please Select Answer		c. Mechanisms and trained specialists to analyse threats, vulnerabilities, and potential impacts which are associated with business activities d. Arrangements to determine and apply cost-effective security controls to mitigate the identified risks within agreed appetites; e. Assurance processes to make sure that mitigations are, and remain effective.	SPF - Culture Awareness ISO27001:2005 - A.10.1 ISO27001:2013 - A.12.1, A9.4	3 - Yes with signed acknowledgement 2 - Yes 0 - No	
3.4 Are access controls in place to ensure information is only available to system users who require access?	Please Select Answer			SPF - Technology & Services ISO27001:2005 - A.11 ISO27001:2013 - A.9, A.11 Cyber Essential:3 User Access Control	3 - Yes with Policy 2 - Yes 0 - No	
3.5 Are acceptable use policies in place which outline the rules for acceptable use of information and assets?	Please Select Answer		For more information please see ISO/IEC 27001	SPF - Culture Awareness ISO27001:2005 - A.7.1.3	3 - Yes 0 - No	
3.6 Are policies and controls in place to ensure the following?			a. Identified if technology and services are Critical National Infrastructure (CNI), and risk manage accordingly: b. Risk-informed security controls which: • Mitigate applicable threats; • Are kept current and actively managed; • Protect against, detect and correct malicious behaviour; • Ensure that critical technology and services are resilient to disruptive challenges such as cyber attacks, and have the means to recover from these.	SPF - Technology & Services		
Boundary protection is in place on all systems with a connection to an un-trusted network.	Please Select Answer			ISO27001:2005 - A.10.6 ISO27001:2013 - A.13.1 Cyber Essentials:1 Boundary Firewalls	3	
Timely patching is applied against known vulnerabilities.	Please Select Answer			ISO27001:2005 - A.12.6.1, A12.4.1 ISO27001:2013 - A.12.5, A.6 Cyber Essentials:5 Patch Management	3	
Systems are protected from malicious and mobile code.	Please Select Answer			ISO27001:2005 - A.10.4 ISO27001:2013 - A.12.2 Cyber Essentials:4 Malware Protection	3	
Software and hardware is locked down to restrict unnecessary services.	Please Select Answer			ISO27001:2005 - A.11.2.2, A11.5.4 ISO27001:2013 - A.9.4.4 Cyber Essentials:2 Secure Configuration	3	
A protective monitoring regime is in place to oversee how ICT systems are used.	Please Select Answer			ISO27001:2005 - A.10.1 ISO27001:2013 - A.12.4	3	
3.7 Are network security boundaries defined and enforced to group users, services and information that require different levels of protection?	Please Select Answer			SPF - Technology & Services ISO27001:2005 - A.11.4.5 ISO27001:2013 - A.13.1 Cyber Essentials:1 Boundary Firewalls	3 - Yes 0 - No	
3.8 In relation to your use of electronic storage media (include removable media), which of the following area are covered by documented policies and procedures?				SPF - Technology & Services ISO27001:2005 - A.10.7 ISO27001:2013 - A.8.3 Cyber Essentials:2 Secure Configuration		
Control	Please Select Answer				1	
Protection	Please Select Answer				1	
Secure use	Please Select Answer				1	
Destruction	Please Select Answer				1	
3.9 Are policies and controls in place to manage the risks of working in non-secure environments?	Please Select Answer			SPF - Technology & Services SPF - Culture Awareness ISO27001:2005 - A.11.7 ISO27001:2013 - A.6.2	5 - No remote working 3 - Yes 0 - No	
3.10 Are back-up copies of information and software taken regularly?	Please Select Answer			SPF - Technology & Services ISO27001:2005 - A.10.5 ISO27001:2013 - A.12.3	5 - Yes Policy tested 3 - Yes 0 - No	
3.11 Has the security of your ICT been evaluated through penetration testing?	Please Select Answer		This should take account of technical vulnerabilities, restrictions to software installation and audit controls to minimise disruptions to business operations.	SPF - Technology & Services ISO27001:2013 - A.12.6	5 - CESG 4 - External Organisation 3 - Cyber Essentials 0 - No	

Questionnaire			Information and Guidance			
Question	**Response**	**Response Comments**	**Question Guidance -** These are examples of the types of controls which maybe appropriate to manage the risks. However this list is not exhaustive. The importance thing here is to ensure the risks are identified and managed at a level which is acceptable to the delivery of the service and aligned to HMG departments risk appetite.	**Corresponding Framework**	**Risk Score/Indicator**	**Critical**
Supplementary. Please use this field to add any additional information that is relevant to this section.	[Free text]					
4.0 Physical & Environmental - This section seeks to determine your approach to physically securing sites used in the delivery of your service, in particular those sites at which our assets are processed or stored. Physical security describes a range of controls that are intended to protect individuals from violence; prevent unauthorised access to sites and / or protectively marked material (and other valuable assets); and reduce the risk of a range of physical threats and mitigate their impact to a level that is acceptable to the organisation. Security must be incorporated into the initial stages of planning, selecting, designing or modifying any building or facility, using appropriate methodologies; putting in place integrated and proportionate control measures to prevent, deter, detect and/or delay attempted physical attacks, and to trigger an appropriate response.						
4.1 Has a review of the security risk assessment been carried out at sites used to process or store our assets in the last 12 months?	Please Select Answer		Appropriate physical security measures will ensure a safe and secure working environment for staff, that can protect against a wide range of threats (including criminality: theft and terrorism or espionage). If the supplier has not completed a risk assessment then the following question which relates to this risk assessment may not need to be completed. Skip 4.2.	SPF - Physical Security Measures and Counter Terrorism ISO27001:2005 - A.9.1 ISO27001:2013 - A.11	3 - Yes 5 - Yes - Annual review 0 - No	Critical
4.2 What areas did the risk assessment cover?			a. Processes and plans in place, including those developed from the early stages of building design, to determine the appropriate physical security requirements through planning and risk assessment; b. Mechanisms to implement internal and external security controls in a layered fashion that deters or prevents unauthorised access and protect assets, especially those that are critical or sensitive against forcible or surreptitious attack; c. Substantial controls for controlling access and proximity to the most high risk sites and Critical National Infrastructure assets.	SPF - Physical Security Measures and Counter Terrorism		
Perimeter Security	Please Select Answer			ISO27001:2013 - A.11.1.1	1	
Access Control	Please Select Answer			ISO27001:2005 - A.9.1.6 ISO27001:2013 - A.11.1.2	1	
Manned Guarding	Please Select Answer			ISO27001:2005 - A.9.1.2	1	
Incoming mail and delivery screening	Please Select Answer			ISO27001:2005 - A.9.1.1 ISO27001:2013 - A.11.1.6	1	
Secure areas and/or cabinets for the storage of sensitive assets.	Please Select Answer			ISO27001:2013 - A.11.1.6	1	
4.3 Which of the following are in place to ensure the physical security controls you have in place are fit for purpose?	Please Select Answer			SPF - Physical Security Measures	3 3	
4.4 Are processes and controls in place to ensure that equipment and cabling is protected and maintained so as to preserve the confidentiality, integrity and availability of our assets?	Please Select Answer		For more information please see ISO/IEC 27001. This includes the requirement for equipment to be maintained in accordance with manufacturers instructions.	SPF - Physical Security Measures ISO27001:2005 - A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6 ISO27001:2013 - A.11.2.1, A11.2.2, A.11.2.3, A.11.2.4, A.11.2.5, A.11.2.6	3 - Yes 0 - No	
Supplementary. Please use this field to add any additional information that is relevant to this section.	[Free text]					
5.0 Personnel & HR - This section seeks to determine your approach to personnel security, security training and awareness programmes and how individual responsibility for security is made clear to your staff. Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. They should be maintained throughout a member of staff's time in employment. Controls should be put in place to ensure that employees understand their personal responsibility to safeguard sensitive assets. As well as to ensure they are adequately screened in order to addresses the risks associated with identity fraud, illegal working and deception generally.						
5.1 Are background verification checks carried out on employees and contractors who have access to our assets?	Please Select Answer		People are an organisation's most important asset, so personnel assurance is fundamental to good security. Government organisations will deliver the appropriate combination of recruitment checks, vetting and on-going personnel security management to be assured, and to remain assured, about their people and to mitigate the risks from well-placed insiders.	SPF - Personnel Security and BPSS Document ISO27001:2005 - A.8.1.2 ISO27001:2013 - A.7.1.1	5 - Yes BPSS 3 - Yes BS 3 - Yes neither standard 0 - No	Critical
5.2 Has a risk assessment been undertaken to determine the need for National Security Vetting (NSV) in specific roles?	Please Select Answer		A risk management approach should be used to determine the appropriate levels of personnel security controls.	SPF - Personnel Security ISO27001:2005 - A.8.1.2 ISO27001:2013 - A.7.1.1	3 - Yes no NVS needed 3 - Yes certain role need NVS 0 - No	
5.3 Do you keep full and up to date personnel security records on all employees in order to review clearance in advance of its expiration?	Please Select Answer		Full and up to date personnel security records on all employees that hold security clearances should be maintained. All National Security Vetting clearances should be formally reviewed according to agreed timescales for each level of clearance.	SPF - Personnel Security ISO27001:2005 - A.8.1.2 ISO27001:2013 - A.7.1.1	3 - Yes 0 - No	

Questionnaire			Information and Guidance			
Question	**Response**	**Response Comments**	**Question Guidance -** These are examples of the types of controls which maybe appropriate to manage the risks. However this list is not exhaustive. The importance thing here is to ensure the risks are identified and managed at a level which is acceptable to the delivery of the service and aligned to HMG departments risk appetite.	**Corresponding Framework**	**Risk Score/Indicator**	**Critical**
5.4 Are organisational and individual responsibilities for information security clearly defined in the terms and conditions of employment contracts?	Please Select Answer		a. An appropriate security governance structure to support the Permanent Secretary, that are properly resourced with individuals who have been appropriately trained. These include: • A Senior Information Risk Owner (SIRO); • A Departmental Security Officer (DSO) who can manage day-to-day protective security; • Information Asset Owners (IAOs) across distinct business units; • Information risk assessment and risk management specialists; • Other specialists relevant and specific to the organisation's needs. b. Board-level oversight of security compliance and auditing processes; c. Arrangements to determine and satisfy themselves that Delivery Partners, service providers and third party suppliers, apply proper security controls too (including List X accreditation for companies handling SECRET assets);	SPF - Good Governance ISO27001:2005 - A.8.1.3 ISO27001:2013 - A.7.1.2	5 - Yes 0 - No	Critical
5.5 Are non-disclosure agreements in place with all staff who have access to our assets?	Please Select Answer			SPF - Information	5 - Yes 0 - No	Critical
5.6 Is a mechanism in place to ensure your employees and contractors receive appropriate information security awareness training upon appointment, and regular updates to organisational policies and procedures, as relevant for their job function?	Please Select Answer		Everyday actions and the management of people, at all levels in the organisation, contribute to good security. A strong security culture with clear personal accountability and a mature understanding of managing risk, responsibility and reputation will allow the business to function most effectively. Government organisations will have: a. A security culture that supports business and security priorities and is aligned to HMG's overarching priorities and the organisation's own appreciation of risk;	SPF - Culture Awareness ISO27001:2005 - A.8.1.2, A.8.2.2 ISO27001:2013 - A.7.2.1, A.7.2.2	5 - Yes 0 - No	Critical
5.7 Regarding your organisations information security training programme, which of the following is accurate?			b. Encourages personal responsibility through the management of and delivery of appropriate security training; c. Processes, systems and incentives to deliver this; d. Mechanisms to drive continuous improvement; tackle poor and inappropriate behaviour; enforce sanctions; and encourage the sharing of best practice.	SPF - Culture Awareness		
All staff are required to complete annual security awareness training.	Please Select Answer				1	
Training is incorporated as part of induction process.	Please Select Answer				1	
Training is integrated as a module into our organisations overarching training programme.	Please Select Answer				1	
Training needs analysis has been undertaken and bespoke training delivered to specific roles.	Please Select Answer				1	
All training includes a form of assessment, poor performance is recorded and followed up on.	Please Select Answer				1	
5.8 Is a disciplinary process in place for employees and contractors who have committed a security breach?	Please Select Answer		Well-tested plans, policies and procedures will reduce organisations' vulnerability to security incidents (especially from the most serious threats of terrorism or cyber attack), but also leaks and other disruptive challenges.d. Effective management structures, policies and procedures for detecting, reporting, responding to and handling incidents, including disciplinary measures that are well communicated and understood by staff; e. Reporting mechanisms to the HMG organisation, of incidents of unauthorised disclosure and breaches of official information, including incidents concerning classified information from foreign governments, agencies or organisations. And to the Information Commissioner's Office, if a serious loss or breach of personal data occurs. a. Business continuity arrangements aligned to Industry standards, to maintain key business services, building resilience and security to facilitate a rapid and effective response to and recovering from incidents	SPF - Culture Awareness ISO27001:2005 - A.8.2.3 ISO27001:2013 - A.7.2.3	3 - Yes 0 - No	
5.9 Upon termination of employment is there a process in place to ensure assets are returned and rights to assets revoked?	Please Select Answer			SPF - Personal Security ISO27001:2005 - A.8..3.1, A.8.3.2, A.8.3.3 ISO27001:2013 - A.7.3.1, A.8.1.4, A.9.2.6	3 - Yes 0 - No	Critical is NO
Supplementary. Please use this field to add any additional information that is relevant to this section.	[Free text]					

Schedule 3 - Cyber Essentials Questionnaire

Questionnaire			Information and Guidance			
Question	**Response**	**Response Comments**	**Question Guidance -** These are examples of the types of controls which maybe appropriate to manage the risks. However this list is not exhaustive. The importance thing here is to ensure the risks are identified and managed at a level which is acceptable to the delivery of the service and aligned to HMG departments risk appetite.	**Corresponding Framework**	**Risk Score/Indicator**	**Critical**
6.0 Organisation - This section seeks to determine whether your approach to information assurance ensures that clear lines of responsibility and accountability are in operation at all levels of your organisation.						
6.1 Does your company have a senior individual responsible for the security of our information within your custody?	Please Select Answer	Contact Name: Role: Email Address:	Effective leadership is a critical component of good security and accountability. The Permanent Secretary (or equivalent) will own the organisation's approach to security and ensure that these issues receive the attention and investment required.	SPF - Good Governance ISO27001:2005 - A.8.1.1 ISO27001:2013 - A.6.1.1	3 - Yes 0 - No	Critical
6.2 Are the security roles and responsibilities of your employees clearly defined and documented in accordance with your organisations information security policy?	Please Select Answer		a. Suppliers should ensure an appropriate security governance structure is in place to support the CEO/Director that are properly resourced with individuals who have been appropriately trained. These could include: • A Senior Information Risk Owner (SIRO); - Senior Responsible for information risks • A Chief Security Officer Security Officer (CSO) who can manage day-to-day protective security; • Information Asset Owners (IAOs) across distinct business units; • Information risk assessment and risk management specialists; • Other specialists relevant and specific to the organisation's needs. b. Board-level oversight of security compliance and auditing processes; c. Arrangements to determine and satisfy themselves that Delivery Partners, service providers and third party suppliers, apply proper security controls too	SPF - Good Governance ISO27001:2005 - A.6.1.3 ISO27001:2013 - A.6.1.1	3 - Yes 0 - No	
6.3 Is a process in place to ensure your organisation is kept up to date on relevant current and emerging;			For more information please see ISO/IEC 27001	SPF - Good Governance ISO27001:2005 - A.6.1.7 ISO27001:2013 - A.6.1.4		
Information security best practice	Please Select Answer				1	
Government policy and legislation	Please Select Answer				1	
Threats and vulnerabilities	Please Select Answer				1	
Technologies	Please Select Answer				1	
6.4 Is a corporate approach to risk management in place which enables the escalation of project risks to programme and/or organisational level risk registers?	Please Select Answer			SPF - Risk Management	3 - Yes 0 - No	
6.5 Is a process in place to manage change to systems i.e. capacity management and separation of testing environments?	Please Select Answer		System performance should be maintained when considering changes to resources and capacity requirements. Development and testing environments should be separated from the operational environment.	SPF - Technology and Services ISO27001:2013 - A.12.1.3, A.12.1.4		
Supplementary. Please use this field to add any additional information that is relevant to this section.	[Free text]					
7.0 Security Policy - An information security policy should outline your organisation's overall approach to the management of information security. This section seeks to understand the depth of your security policy and your approach to review.						
7.1 Is a security policy in place setting out your organisation's overall approach to protecting valuable assets?	Please Select Answer		b. A clearly-communicated set of security policies and procedures, which reflect business objectives to support good risk management If the supplier does not have a Security Policy, then the following question which probes the contents of the Security Policy, may not need to be responded to. Skip 7.2	SPF - Risk Management ISO27001:2005 - A.5.11 ISO27001:2013 - A.5.11	5 - Yes 0 - No	Critical
7.2 Does the security policy reference:			For more information please see ISO/IEC 27001	SPF - Culture Awareness ISO27001:2005 - A.5.11 ISO27001:2013 - A.5.11		
The importance of security to your organisation	Please Select Answer				1	
Legislation and regulation that your organisation is required to be compliant with	Please Select Answer				1	
Staff responsibilities for information	Please Select Answer				1	
Incident and breach management policies	Please Select Answer				1	
Business continuity arrangements	Please Select Answer				1	
Staff training & awareness requirements.	Please Select Answer				1	

Questionnaire			Information and Guidance			
Question	**Response**	**Response Comments**	**Question Guidance -** These are examples of the types of controls which maybe appropriate to manage the risks. However this list is not exhaustive. The importance thing here is to ensure the risks are identified and managed at a level which is acceptable to the delivery of the service and aligned to HMG departments risk appetite.	**Corresponding Framework**	**Risk Score/Indicator**	**Critical**
7.3 Has your security policy;				SPF - Risk Management SPF - Good Governance SPF - Culture Awareness ISO27001:2005 - A.5.12 ISO27001:2013 - A.5.12		
been reviewed in the last 12 months?	Please Select Answer				1	
been approved by the senior management?	Please Select Answer				1	
been made accessible to all staff?	Please Select Answer				1	
Supplementary. Please use this field to add any additional information that is relevant to this section.	[Free text]					
8.0 Asset Management - This section seeks to determine your approach to the management of sensitive assets to ensure they are handled, stored, transmitted and destroyed in a manner that is commensurate with the impact of a compromise to their confidentiality, integrity or availability.						
8.1 Is a process in place to ensure assets are classified according to their value and in line with Government classification policy?	Please Select Answer		Mechanisms and processes to ensure assets are properly classified and appropriately protected;	SPF - Information ISO27001:2005 - A.7.1.2 ISO27001:2013 - A.8.2	3 - Yes Gov Classification 3 - Yes In house 3 - No, retain Gov markings 0 - No	
8.2 Has an owner been assigned to all information assets which require protection?	Please Select Answer		An Information Asset Owner should be identified for each of the information assets identified within your organisation's list of information assets and that person should take full and effective responsibility for managing the protection and exploitation of the information for which he/she is responsible. Where the asset is owned by Government it will be valued according to the Government's classification policy. The responsibility for protection of Government assets in your custody should still be assigned to a named individual within your organisation.	SPF - Good Governance and Information ISO27001:2005 - A.7.1.2 ISO27001:2013 - A.8.2	3 - Yes 0 - No	
8.3 Is an asset register in place that identifies and records the value of sensitive assets which require protection?	Please Select Answer		Information and other assets should be valued so as to ensure they are appropriately handled shared and protected. This includes not taking equipment off-site without authorisation.	SPF - Information ISO27001:2005 - A.7.1.1 ISO27001:2013 - A.8.2	5 - Yes 0 - No	Critical
8.4 Do you have policies in place which detail how our assets should be;			Policies, procedures and controls should be in place to ensure information assets are identified, valued, handled, stored, processed, transmitted (including use of electronic messaging), shared and destroyed in accordance with legal requirements and (in the case of Government assets) in line with the standards set out in the Government's classification policy. This should includes protection of assets when off-site and the need for clear desk policies. All assets should be returned by employees on termination of employment. If the supplier does not have policies that govern how Departmental assets should be managed then the following question, which relates to the communication of these policies, may not need to be responded to. Skip 8.5 if no option is selected.	SPF - Information ISO27001:2005 - A.9.1.5, A.7.2.2, A.9.2.6 ISO27001:2015 - A.8.2, A.13.2, A.11.2.6, A.8.1.4		
handled	Please Select Answer				1	Critcial if No
copied	Please Select Answer				1	Critical if No
stored	Please Select Answer				1	Critical if No
transmitted	Please Select Answer				1	Critical if No
destroyed	Please Select Answer				1	Critical if No
returned	Please Select Answer				1	Critical if No
8.5 How are these procedures communicated to staff?	Please Select Answer			SPF - Culture and Awareness ISO27001:2005 - A.5.1.1 ISO27001:2013 - A.5.1.1	1	
Supplementary. Please use this field to add any additional information that is relevant to this section.	[Free text]					
9.0 Incident Management - This section seeks to determine your approach to the management of sensitive assets to ensure they are handled, stored, transmitted and destroyed in a manner that is commensurate with the impact of a compromise to their confidentiality, integrity or availability.						
9.1 Do you have policies in place which set out how information security incidents, and breaches to the confidentiality of data, should be managed and who it should be escalated to?	Please Select Answer		Organisation should have clear policies and processes for reporting, managing and resolving Information Security Breaches and ICT security incidents. Put in place a security incident policy setting out clear guidance for staff on the potential disciplinary and / or criminal penalties that may result from failure to comply with security policies. If the supplier does not have an Incident Management Policy, then the following question which probes the contents of this policy, may not need to be responded to. Skip 9.2.	SPF - Preparing for and responding to Security Incidents ISO27001:2005 - A.13.2.1 ISO27001:2013 - A.16.1	5 - Yes 0 - No	Critical
9.2 Do these policies make reference to the following?						
Individual responsibilities for identifying and reporting security incidents and information security breaches	Please Select Answer			SPF - Preparing for and responding to Security Incidents ISO27001:2005 - A.13.2.1 ISO27001:2013 - A.16.1	1	
A reporting matrix including escalation points	Please Select Answer				1	

Questionnaire			Information and Guidance			
Question	**Response**	**Response Comments**	**Question Guidance -** These are examples of the types of controls which maybe appropriate to manage the risks. However this list is not exhaustive. The importance thing here is to ensure the risks are identified and managed at a level which is acceptable to the delivery of the service and aligned to HMG departments risk appetite.	**Corresponding Framework**	**Risk Score/Indicator**	**Critical**
An up to date list of relevant internal and external contact points	Please Select Answer				1	
A timeline detailing at which point the policy should be implemented	Please Select Answer				1	
9.3 In the event of a loss or breach to one of our assets which of the following actions would your organisation take first;	Please Select Answer			SPF - Preparing for and responding to Security Incidents ISO27001:2013 - A.16.1	0 - Rectify breach 0 - Determine loss 5 - Report Incident	
9.4 Is a forensic readiness policy in place documenting your approach to managing digital evidence relating to ICT security incidents?	Please Select Answer		It is important for each organisation to develop a Forensic Readiness of sufficient capability and that it is matched to its business need. Readiness involves specification of a policy that lays down a consistent approach, detailed planning against typical (and actual) case scenarios that an organisation faces, identification of (internal or external) resources that can be deployed as part of those plans, identification of where and how the associated Digital Evidence can be gathered that will support case investigation and a process of continuous improvement that learns from experience.	SPF - Preparing for and responding to Security Incidents ISO27001:2005 - A.13.2.3 ISO27001:2013 - A.16.1.6	3 - Yes 5 - Yes specific reference 0 - No	
Supplementary. Please use this field to add any additional information that is relevant to this section.	[Free text]					
10.0 Business Continuity - This section seeks to determine whether or not effective Business Continuity Management (BCM) in place to plan how to maintain those parts of your organisation that you can't afford to lose if an incident occurs.						
10.1 Does your organisation have business continuity and disaster recovery plans in place to maintain or quickly resume any services you provide to us?	Please Select Answer		A business continuity management system to enable you to maintain or else quickly resume provision of key services in the event of a disruption should be put in place. Business continuity management arrangements should follow industry best practice (BS25999 or equivalent standard). If the supplier does not have a BC plan then the following question which probes the testing and review of this plan, may not need to be responded to. Skip 10.2.	SPF - Preparing for and responding to Security Incidents ISO27001:2005 - A.14.1.1 ISO27001:2013 - A.17.1.1, A.17.1.2	5 - Yes comply BS 3 - Yes 0 - No	Critical
10.2 Are processes in place to ensure business continuity management arrangements are tested and reviewed?	Please Select Answer		BCM arrangements should be tested and reviewed at least annually or following significant organisational change.	SPF - Preparing for and responding to Security Incidents ISO27001:2005 - A.14.1.5 ISO27001:2013 - A.17.1.3	5 - Yes tested & reviewed 3 - Yes not tested 3 - No formal process 0 - No	
Supplementary. Please use this field to add any additional information that is relevant to this section.	[Free text]					
11.0 Compliance - This section seeks to determine your approach to ensuring both you and your subcontractors, are compliant with our security policy and associated legislation and regulation.						
11.1 How does your organisation ensure that relevant legislation and regulation is understood?			For more information please see ISO/IEC 27001	SPF - Culture and Awareness ISO27001:2005 - A.15.1.1 ISO27001:2013 - A.16.1		
Contact with relevant authorities is maintained	Please Select Answer				1	
All changes are reviewed to determine the impact for your business	Please Select Answer				1	
Relevant legislation and regulation is referenced in internal policies, plans and procedures.	Please Select Answer				1	
11.2 Does your company provide guidance to staff on handling our information with respect to?			All staff handling sensitive government assets should be briefed about how legislation (particularly the OSA, FOIA and DPA) specifically relates to their role, including the potential disciplinary or criminal penalties that may result from failure to comply with security policies.	SPF - Culture and Awareness ISO27001:2013 - A.7.2.2		
Data Protection Act	Please Select Answer				1	
Freedom of Information Act	Please Select Answer				1	
Official Secrets Act	Please Select Answer				1	
Environmental Information Act	Please Select Answer				1	
11.3 In the past 12 months has your organisation assessed its compliance with relevant legislation and regulation (for example the Data Protection Act)?	Please Select Answer			SPF - Technology and Services ISO27001:2013 - A.18.2.2	5 - Yes no weakness 5 - Yes action plan 3 - Yes no plan 0 - No	
11.4 In the past 12 months have your organisation's information security controls, policies and procedures, been independently reviewed?	Please Select Answer		For more information please see ISO/IEC 27001	SPF - Risk Management & Technology and Services ISO27001:2005 - A.6.1.8 ISO27001:2013 - A.18.2.1	5 - Yes 3 - No Internal Review 0 - No	

Questionnaire			Information and Guidance			
Question	**Response**	**Response Comments**	**Question Guidance -** These are examples of the types of controls which maybe appropriate to manage the risks. However this list is not exhaustive. The importance thing here is to ensure the risks are identified and managed at a level which is acceptable to the delivery of the service and aligned to HMG departments risk appetite.	**Corresponding Framework**	**Risk Score/Indicator**	**Critical**
11.5 Are processes in place to ensure that you assess the risks to assets that are shared with your delivery partners and third party suppliers?	Please Select Answer		Organisations should ensure that the security arrangements among their wider family of delivery partners and third party suppliers are appropriate to the information concerned and the level of risk . This must include appropriate governance and management arrangements to manage risk, monitor compliance and respond effectively to any incidents.	SPF - Risk Management ISO27001:2013 - A.15.1	5 - Yes 0 - No	Critical
11.6 How does your company gain assurance that delivery partners and third party suppliers are compliant with your security policies?			Organisations should ensure that they seek assurance from their delivery partners and third party suppliers to ensure that they are managing their protective security and information risks to an appropriate level. This should include working closely with security, procurement and contract management teams to ensure that adequate security, information assurance and business continuity requirements are specified in contracts with third party suppliers.	SPF - Risk Management ISO27001:2013 - A.15.1		
Information security requirements are detailed in contracts	Please Select Answer				3	Critical
Your right to audit is detailed in contracts and is exercised	Please Select Answer				3	
The need to meet recognised standards (such as ISO27001:2013) is stipulated	Please Select Answer				1	
The organisations compliance is measured through self-assessment	Please Select Answer				1	
Supplementary. Please use this field to add any additional information that is relevant to this section.	[Free text]					

for and on behalf of [**THE SUPPLIER]**

Signed .....

Name …….

Position …….

Date …….

for and on behalf of [**THE CUSTOMER]**

Signed .....

Name …….

Position …….

Date …….

THIS IS THE LAST PAGE OF THESE TERMS & CONDITIONS