



Foreign, Commonwealth  
& Development Office

## **CONTRACT DOCUMENT**

**Project 9629 / ITT 5816**

**Hardship and Cost of Living Data Processing & Provision**

**SECTION 1: FORM OF CONTRACT**

THIS CONTRACT is made between the Secretary of State for Foreign, Commonwealth & Development Affairs represented by the Foreign, Commonwealth & Development Office, acting as part of the Crown ("the Authority"),

and

ECA International ("the Contractor") having his main or registered office at New Brook Buildings, 16 Great Queen Street, London, WC2B 5DG

("the Parties")

IT IS AGREED THAT:

1. This Form of Contract (Section 1) together with the attached Sections 2 to 6 inclusive are the documents which collectively form "the Contract" (as defined in Section 2).

Section 1	Form Of Contract
Section 2	FCDO Conditions of Contract & Appendices
Section 3	Statement of Service Requirements
Section 4	Schedule of Prices & Rates
Section 5	NOT USED
Section 6	Successful Tenderers Response to ITT

2. The Contract effected by the signing of this Form of Agreement constitutes the entire agreement between the Parties relating to the subject matter of the Contract and supersedes all prior negotiations, representations or understandings whether written or oral.

SIGNED on behalf of the Parties:

For the Contractor:

For the Authority:

By: .....

By:

Full Name: .....

Full Name:

Position held on behalf of Contractor:

Position held on behalf of Authority:

Date:

Date:

Index of Contract Conditions

A.	<u>General Provisions</u>	F	<u>Control of the Contract</u>
A1	Definitions and Interpretation	F1	Transfer and Sub-Contracting
A2	Initial Contract Period	F2	Waiver
A3	Contractor's Status	F3	Variation
A4	Authority's Obligations	F4	Severability
A5	Notices	F5	Inadequate Performance Remedies
A6	Mistakes in Information	F6	Remedies Cumulative
A7	Conflicts of Interest	F7	Monitoring of Contract Performance
B.	<u>Supply of Services</u>	F8	Entire Agreement
B1	The Services	F9	Subcontract opportunities for SMEs and VCSEs – NOT USED
B2	Provision and Removal of Equipment – NOT USED	F10	Management Changes and Information – NOT USED
B3	Manner of Carrying Out the Services	F11	Financial Distress
B4	Key Personnel	G	<u>Liabilities</u>
B5	Contractor's Staff – NOT USED	G1	Liability, Indemnity and Insurance
B6	Inspection of Premises	G2	Professional Indemnity
B7	Licence to Occupy Premises – NOT USED	G3	Warranties and Representations
B8	Property – NOT USED	H	<u>Default, Disruption and Termination</u>
B9	Offers of Employment	H1	Termination on Insolvency, Change of Control
B10	Meetings and Reports	H2	Termination on Default
B11	Safeguarding	H3	Break
C.	<u>Payment and Contract Price</u>	H4	Consequences of Expiry or Termination
C1	Contract Price	H5	Disruption
C2	Payment and VAT	H6	Recovery upon Termination
C3	Recovery of Sums Due	H7	Force Majeure
C4	Price Adjustment	H8	Exit Management
C5	Euro	I	<u>Disputes and Law</u>
D.	<u>Statutory Obligations and Regulations</u>	I1	Governing Law and Jurisdiction
D1	Prevention of Corruption	I2	Dispute Resolution
D2	Prevention of Fraud	K	<u>Category Specific Questions – NOT USED</u>
D3	Discrimination	K1	Commencement of full operations – NOT USED
D4	The Contracts (Rights of Third Parties) Act 1999	K2	Co-ordination – NOT USED
D5	Environmental Requirements	K3	Responsibility for equipment – NOT USED
D6	Health and Safety – NOT USED	K4	Title and risk – NOT USED
D7	Transfer of Undertakings Regs 2006	K5	Acceptance – NOT USED
E.	<u>Protection of Information</u>	K6	Flexible operations – NOT USED
E1	Data Protection		
E2	Official Secrets Acts 1911, 1989, S182 of the Finance Act 1989		
E3	Confidential Information		
E4	- Not Used -		
E5	Publicity, Media and Official Enquiries		
E6	Security		
E7	Intellectual Property Rights		
E8	Audit		
E9	Authority Data		
E10	Removable Media – NOT USED		
E11	Transparency		

Appendix

- A Variation to contract form
- B Confidentiality undertaking
- C Key staff
- D Commercially sensitive information
- E Code of conduct for private security companies and private security service providers – NOT USED
- F Call off instruction – NOT USED
- G.1 Schedule of Processing, Personal Data and Data Subjects
- G.2 Joint Controllers Agreement – NOT USED
- H Supplier Code of Conduct
- I Supplier Business Continuity and Disaster Recovery Plan

**Col. A****LONG CONTRACT CONDITIONS****A. GENERAL PROVISIONS**

(1) NOT USED

(2) NOT USED

**A1. DEFINITIONS AND INTERPRETATION**

In these Conditions, unless the context otherwise requires, the following provisions shall have the meanings given to them below:

"ADR Notice" means a notice served under Condition I2 (Dispute Resolution) requesting mediation.

"Affiliate" means in relation to a body corporate, any other entity which directly or indirectly controls, is controlled by, or is under direct or indirect common control with, that body corporate from time to time.

"Agreement" means this contract

"Approval" and "Approved" refer to the written consent of the Authority's Representative. (Conditions B3.1.1, E1.4, F1.1, F1.7, F11.3, F11.5, F11.7, F11.9, H1.3, H5.3 refer.)

"Authority" means the Secretary of State for Foreign, Commonwealth and Development Affairs and includes the Authority's Representative. In this Contract, the Authority is acting as part of the Crown.

"Authority Data" means (a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Authority; or (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Agreement; or (b) any Personal Data for which the Authority is the Data Controller.

"Authority's Representative" means the individual authorised to act on behalf of the Authority for the purposes of the Contract.

"Authority Software" means software which is owned by or licensed to the Authority, including software which is or will be used by the Contractor for the purposes of providing the Services but excluding the Contractor Software.

"Commencement of Full Operations" means the point in time when the Contractor becomes responsible for the provision of the Services following the completion of the Setting up Operations defined in the KEY MILESTONES section of the Statement of Service Requirements. In the event that the Contractor's responsibility for the provision of the Services is phased, the Commencement of Full Operations means the commencement of each phase following the Setting Up Operations in respect of that phase.

"Commencement Date" means the date when the period of the duration of the contract commences in accordance with Condition A2 (Initial Contract Period).

"Commercially Sensitive Information" means the subset of Confidential Information listed in Appendix D comprised of information:

- (a) which is provided by the Contractor to the Authority in confidence for the period set out in that schedule; and/or
- (b) that constitutes a trade secret.

"Condition" means a condition or clause within the Contract.

"Confidential Information" means any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information the disclosure of which would, or would be likely to, prejudice the commercial interests of any person, trade secrets, Intellectual Property Rights and know-how of either Party and all personal data and sensitive personal data within the meaning of the DPA. Confidential Information shall not include information which:

- (i) was public knowledge at the time of disclosure (otherwise than by breach of Condition E3 (Confidential Information));
- (ii) was in the possession of the receiving Party, without restriction as to its disclosure, before receiving it from the disclosing Party;
- (iii) is received from a third party (who lawfully acquired it) without restriction as to its disclosure; or
- (iv) is independently developed without access to the Confidential Information.

"Contract" means this agreement between the Authority and the Contractor consisting of these Conditions, Sections, attached Schedules and Appendices and the Contractor proposal reference (Section 6) dated 22 September 2023/16 October 2023 (for the presentation).

"Contractor" means ECA International

"Contractor's Representative" means the individual authorised to act on behalf of the Contractor for the purposes of the Contract.

"Contractor Software" means software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services.

"Contract Period" means the period of the duration of the Contract in accordance with Condition A2 (Initial Contract Period).

"Contractor Personnel" means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any Sub-Contractor engaged in the performance of its obligations under this Agreement

"Contract Price" means the price, exclusive of any applicable Value Added Tax, payable by the Authority to the Contractor, as set out in Condition C1 (Contract price).

"Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer" take the meaning given in the GDPR.

"Credit transfer" is a payment instruction from the Authority to its bank or payment service provider to transfer an amount of money to another account.

"The Crown" means any central government department of the United Kingdom, or a Devolved Administration, or any other body which is legally defined as a Crown Body.

"DPA 2018" means the Data Protection Act 2018

"Data Protection Legislation" means

- (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time

- (ii) the DPA 2018 [subject to Royal Assent] to the extent that it relates to processing of personal data and privacy;
- (iii) all applicable Law about the processing of personal data and privacy;

"Data Protection Impact Assessment" an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

"Data Loss Event" means any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

"Data Subject Request" means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

"DPA 2018" means the Data Protection Act 2018

"Default" means any breach of the obligations of either Party (including but not limited to fundamental breach or breach of a fundamental item) or any default, act, omission, negligence or statement of either Party, its employees, contractors, agents or Sub-Contractors in connection with or in relation to the subject matter of this Contract and in respect of which such Party is liable to the other.

"Effective Date" means the date when the contract legally commences.

"Equality Enactments" means the enactments defined in section 33(1) Equality Act 2006.

"Equipment" means all equipment, materials, consumables and plant and other items supplied, other than Authority's Property, to be used by the Staff in the provision of the Services.

"Environmental Information Regulations" means the Environmental Information Regulations 2004, as the same may be amended or updated 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 regulations.

"FOIA" means the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner in relation to such legislation.

"Force Majeure" has the meaning set out in Condition H7 (Force Majeure).

"GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679)

"Good Industry Practice" means at any time the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced provider of services similar to the Services seeking in good faith to comply with its contractual obligations and complying with all relevant laws.

"Goods" means anything which the Contractor supplies to the Authority under the Contract including any materials provided as part of the Service;

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

"Intellectual Property Rights" means patents, inventions, trademarks, service marks, logos, design rights (whether registerable or not), applications for any of the above rights, copyright, database rights, domain names, know how, trade or business names, moral rights or other similar rights or obligations whether registerable or not in any country including but not limited to the United Kingdom.

"Joint Controllers" means where two or more Controllers jointly determine the purposes and means of processing

"Key Performance Indicators" means a set of quantifiable measures that the Authority and Contractor will use to measure the performance of the Services provided by the Contractor under the Contract.

"Key Staff" means all persons identified in Appendix C – Key Staff.

"LED" means Law Enforcement Directive (Directive (EU) 2016/680)

"Law" means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply;

"Malicious Software" means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.

"Month" means calendar month.

"Notice" means information from either Party to the other Party about a particular action that has been taken;

"Party" means either the Authority or the Contractor and the "Parties" means the Authority and the Contractor;

"Personnel" means persons directly employed by the Authority.

"Premises" means land or buildings where the Services are performed.

"Price" means a price entered in Section 3 - Schedule of Prices and Rates

"Processor Personnel" means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Agreement

"Proposal" means the Contractor's proposal submitted to the Authority to meet the requirement detailed in the Authority's tender documentation or request for quotation dated 24 July 2023 and any subsequent clarifications dated 30 August 2023.

"Protective Measures" means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in Schedule [x] (Security).



"Purchase Order" or "PO" means the form, which the Authority sends to the Contractor confirming the contract and facilitating payment via the Authority Purchase to Pay System;

"Rates" means a rate entered in Section 3 - Schedule of Prices and Rates

"Regulatory Bodies" means those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Contract or any other affairs of the Authority and "Regulatory Body" shall be construed accordingly.

"Requests for Information" shall have the meaning set out in the FOIA or any apparent request for information under the FOIA or the Environmental Information Regulations as relevant.

"Security Policy" means the Authority's ICT security policy provided by the Authority and updated from time to time.

"Setting Up Operations" means the period of time, or periods of time where phased, as detailed in the KEY MILESTONES section of the Statement of Service Requirements, during which the Contractor is required to mobilise itself and its Staff in preparation for delivering the Service and for the Commencement of Full Operations.

"Services" means all the services (including any works) which the Contractor provides to the Authority under the Contract.

"Staff" means all persons used by the Contractor to deliver the contract.

"Sub-contractor" means any third party employed by the Contractor in the provision of the Services.

"Sub-processor" any third Party appointed to process Personal Data on behalf of the Contractor related to this Agreement

"Successor Supplier" means the Authority or a replacement contractor who takes over responsibility for all or part of the Services following expiry, termination or partial termination of the Contract.

"Termination Transfer" means the transfer of responsibility for delivery of the Contract from the Contractor to the Authority and/or a Successor Supplier on or following the termination or expiry of this Contract or any part thereof.

"Termination Transfer Date" means the date of a Termination Transfer.

"Termination Transfer Employees" means the Staff employed immediately before the Termination Transfer Date by the Contractor or any of its sub-contractors and who are providing the Services(s) to be transferred on the Termination Transfer Date (and to be carried out in the same, equivalent or broadly similar way after the Termination Transfer Date) and whose names are included in the list of transferring staff provided by the Contractor, less any person so listed whose employment with the Contractor or any of its sub-contractors ends prior to the Termination Transfer; and less any person so listed whose employment does not transfer pursuant to and by virtue of Regulations 4(7) and 4(8) of The Transfer Of Undertakings (Protection Of Employment) Regulations 2006 (employees objecting to employment transferring).

"the Crown" means any central government department of the United Kingdom, including the Devolved Administrations, and other bodies which are legally defined as being Crown Bodies.

"TUPE Regulations" means the Transfer of Undertakings (Protection of Employment) Regulations 2006 (as amended).

"Variation" means a properly executed variation to the Contract in compliance with Condition F3 (Variation).

“Variation to Contract Form” means the form set out in Appendix A - Variation to Contract Form.

“Working Day” means any day other than a Saturday, Sunday or public holiday in England and Wales.

#### A1.1. FURTHER PROVISIONS

The interpretation and construction of the Contract shall be subject to the following provisions:

- a) a reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as subsequently amended or re-enacted;
- b) the headings included in the Contract are for ease of reference only and shall not affect the interpretation or construction of the Contract;
- c) references to Conditions are references to Conditions in the Conditions of the Contract in which they appear, unless otherwise stated;
- d) where the context allows, the masculine includes the feminine and the neuter, and the singular includes the plural and vice versa;
- e) reference to a Condition is a reference to the whole of that Condition unless stated otherwise;
- f) reference to any person shall include natural persons and partnerships, firms and other incorporated bodies and all other legal persons of whatever kind and however constituted and their successors and permitted assigns or transferees; and
- g) any words following the terms including, include, in particular or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or terms preceding those terms and the words “include”, “includes” and “including” are to be construed as if they were immediately followed by the words “without limitation”.
- h) These Conditions shall apply to the exclusion of all other terms and conditions including any terms and conditions which the Contractor may seek to apply under any purchase order, confirmation of order, invoice, delivery note or similar document.
- i) The Contractor shall be deemed to have accepted the terms and conditions of the Contract by delivering the Goods and/or Service.
- j) Time for delivery of Goods and/or provision of the Service shall be of the essence of the Contract.
- k) If either Party does not enforce any one or more of the terms or conditions of this Contract this does not mean that the Party has given up the right at any time subsequently to enforce all terms and conditions of this Contract.
- l) Neither party shall be liable for any claim, loss or damage whether arising in contract, tort (including negligence) or otherwise, for consequential, economic, special or other indirect loss and shall not be liable for any losses calculated by reference to profits, contracts, business, goodwill, income, production or accruals whether direct or indirect and whether or not arising out of any liability of the Contractor to any other person.

#### A2. CONTRACT PERIOD

- A2.1 The Contract period begins on Monday 15 April 2024 and ends on Saturday 14 April 2029. The Parties may extend the Contract by 2 further periods of 12 months, up to Monday 14 April 2031. Any extensions to the Contract period shall be mutually agreed between Authority and Contractor and confirmed in writing in accordance with Condition F3 of the contract.

#### A3. CONTRACTOR'S STATUS

- A3.1 At all times during the Contract Period, the Contractor shall be an independent contractor and nothing in this Contract shall create a contract of employment, a relationship of agency or partnership or joint venture between the Parties and accordingly neither Party shall be authorised to act in the name of, or on behalf of, or otherwise bind the other Party save as expressly permitted by the terms of this Contract accordingly:
  - a) the Contractor shall not say or do anything that might lead any other Person to believe that the Contractor is acting as the agent of the Authority; and

- b) the Authority shall not incur any contractual liability to any other Person as a result of anything done by the Contractor in connection with the performance of the Contract.
- A4. AUTHORITIES OBLIGATIONS
- A4.1 Save as otherwise expressly provided, the obligations of the Authority under the Contract are obligations of the Authority in its capacity as a contracting counterparty and nothing in the Contract shall operate as an obligation upon, or in any other way fetter or constrain the Authority in any other capacity, nor shall the exercise by the Authority of its duties and powers in any other capacity lead to any liability under the Contract (howsoever arising) on the part of the Authority to the Contractor.
- A5. NOTICES
- A5.1 Except as otherwise expressly provided within this Contract, no communication from one Party to the other shall have any validity under this Contract unless made in writing by or on behalf of the Party concerned.
- A5.2 Any notice or other communication which is to be given by either Party to the other shall be given by letter or electronic mail. Such letters shall be addressed to the other Party in the manner referred to in Condition A5.3 (Notices). If the other Party does not acknowledge receipt of any such letter or item of electronic mail, and, in the case of a letter, the relevant letter is not returned as undelivered, the notice or communication shall be deemed to have been given 3 Working Days after the day on which the letter was posted.
- A5.3 For the purposes of Condition A5.2 (Notices), the address of each Party shall be:
- a) The Authority's Representative:
- |                  |   |   |
|------------------|---|---|
| Name             | - | [REDACTED]  |
| Telephone Number |   | [REDACTED]  |
| Address          |   | Foreign, Commonwealth & Development Office, King Charles Street, London, SW1A 2AH |
| E-Mail Address   | - | [REDACTED]  |
| Name             | - | [REDACTED]  |
| Telephone Number |   | [REDACTED]  |
| Address          |   | Foreign, Commonwealth & Development Office, King Charles Street, London, SW1A 2AH |
| E-Mail Address   | - | [REDACTED]  |
| E-Mail Address   | - | [REDACTED]  |
- b) The Contractor's Representative:
- |                  |   |   |
|------------------|---|---|
| Name             | - | [REDACTED]  |
| Telephone Number |   | [REDACTED]  |
| Address          |   | ECA International, 2 <sup>nd</sup> Floor New Brook Buildings, 16 Great Queen Street, London, WC2B 5DG |
| E-Mail Address   | - | [REDACTED]  |
- A5.4 Either Party may change its address for service by notice given in accordance with this Condition A5 (Notices).
- A6. MISTAKES IN INFORMATION
- A6.1 Both parties accept and acknowledge that the formulae involved in calculating indices are subjective and the Contractor shall use reasonable endeavours to ensure the accuracy of all drawings, documentation and information supplied to the Authority by the Contractor in connection with the supply of the Services.
- A7. CONFLICTS OF INTEREST

- A7.1 The Contractor shall establish and maintain appropriate business standards, procedures and controls to ensure that no conflict of interest arises between the Parties, howsoever arising.
- A7.2 The Contractor shall notify the Authority immediately of any circumstances of which it becomes aware which give rise or potentially give rise to a conflict with the Services and shall advise the Authority of how they intend to avoid such a conflict arising or remedy such situation. The Contractor shall subject to any obligations of confidentiality it may have to third parties provide all information and assistance reasonably necessary (at the Contractor's cost) that the Authority may request of the Contractor in order to avoid or resolve a conflict of interest and shall ensure that at all times they work together with the Authority with the aim of avoiding a conflict or remedy a conflict.
- A7.3 The Authority reserves the right to terminate this contract immediately by notice in writing and/or to take such steps it deems necessary where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Contractor and the duties owed to the Authority under the provisions of this contract. The actions of the Authority pursuant to this Article will not prejudice or affect any right of action or remedy which will have accrued or will thereafter accrue to the Authority.
- A7.4 In addition to its obligations under Condition E5 (Publicity, Media and Official Enquiries), the Contractor shall:
- (a) Avoid expressing views which may prejudice the position of the Authority;
  - (b) Make clear when it is expressing views on behalf of the Authority and/or the Government of the United Kingdom, and when it is expressing personal views;
  - (c) Check with the Authority first if they are unsure whether expressing views might be caught by (a) and (b); and
  - (d) Not carry out any acts on behalf of third parties in the course of performing the Services, without the Authority's permission.
- A7.5 Pursuant to Condition A7.2 (Conflict of Interest), the Authority shall have the right to require that the Contractor puts in place "Ethical Walls" and will ensure and satisfy the Authority that all information relating to the Contract and to the Services and Deliverables completed pursuant to it (to include all working papers, draft reports in both tangible and intangible form) are not shared or made available to other employees, contractors or agents of the Contractor and that such matters are not discussed by the relevant staff with other employees, contractors or agents of the Contractor.
- A7.6 NOT USED
- A7.7 NOT USED
- B. SUPPLY OF SERVICES AND/OR GOODS
- B1. THE SERVICES/GOODS
- B1.1 The Contractor shall perform the Services in the manner and exercising that degree of skill, care, diligence, which would reasonably and ordinarily be expected from a skilled and experienced person engaged in providing the same or similar services as the Contractor in the same or similar circumstances as are relevant for the purposes of the Contract.
- B1.2 Where no delivery time is specified by the Authority the Services shall be provided within 10 working days of receipt of the order by the Contractor unless otherwise agreed between the parties.
- B1.3 The Contractor shall make good at its own expense any defects in the Service and/or workmanship which exist or may appear up to 6 months after completion of the Service.
- B1.4 Where applicable, the Contractor must provide the Authority with a copy of its insurance certificate under the Construction Industry Tax Deduction Scheme before commencing the Services.
- B2. PROVISION AND REMOVAL OF EQUIPMENT – NOT USED
- B3. MANNER OF CARRYING OUT THE SERVICES
- B3.1 The Contractor shall at all times comply with the Quality Standards identified in the Statement of Service Requirements, and where applicable shall maintain accreditation with the relevant Quality Standards authorisation body. To the extent that the standard of Services has not been specified in the Contract, the Contractor shall agree the relevant standard of the Services with the Authority prior to the supply of the

Services and, in any event, the Contractor shall perform its obligations under the Contract in accordance with the Law and Good Industry Practice.

- B3.1.1 On the request of the Authority's Representative, the Contractor shall provide proof to the Authority's satisfaction that the materials and processes used, or proposed to be used, conform to the Quality Standards identified in the Statement of Service Requirements. The introduction of new methods or systems which impinge on the provision of the Services shall be subject to prior Approval.
- B3.2 The Contractor shall ensure that all Staff supplying the Services shall do so with all due skill, care and diligence and shall possess such qualifications, skills and experience as are necessary for the proper supply of the Services.
- B3.3 NOT USED
- B3.4 The Contractor shall upon the instruction of the Authority's Representative:
- a) NOT USED
  - b) remove and properly execute any work which is not in accordance with the Contract, irrespective of any previous testing or payment by the Authority. The Contractor shall at its own expense complete the re-executed work correctly in accordance with the Contract within such reasonable time as the Authority may specify.
- B3.5 The signing by the Authority's Representative of time sheets or other similar documents shall not be construed as implying the Contractor's compliance with the Contract.
- B3.6 NOT USED
- B4. KEY PERSONNEL
- B4.1 The Contractor acknowledges that the Key Personnel identified in Appendix C are essential to the proper provision of the Services to the Authority. All Key Personnel and other Personnel deployed on work relating to this Contract shall be appropriately qualified. The Contractor shall supervise and manage all such Personnel properly.
- B4.2 The Key Personnel shall not be released from supplying the Services without the agreement of the Authority, except by reason of long-term sickness, maternity leave, paternity leave or termination of employment and other extenuating circumstances.
- B4.3 Any replacements to the Key Personnel shall be subject to the agreement of the Authority. Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.
- B4.4 The Authority shall not unreasonably withhold its agreement under Conditions B4.2 or B4.3. Such agreement shall be conditional on appropriate arrangements being made by the Contractor to minimise any adverse impact on the Contract which could be caused by a change in Key Personnel.
- B5. CONTRACTOR'S STAFF – NOT USED
- B6. INSPECTION OF PREMISES
- B6.1 The Services shall be subject to inspection at all times by the Authority's Representative and shall be done to a standard considered reasonable by it. The Contractor warrants that it has the experience and capability to execute the Services in a manner satisfactory to the Authority and in accordance with the Conditions of this Contract.
- B7. LICENCE TO OCCUPY PREMISES – NOT USED
- B8. PROPERTY – NOT USED
- B9. OFFERS OF EMPLOYMENT
- B9.1 For the duration of the Contract and for a period of 12 months thereafter neither the Authority nor the Contractor shall employ or offer employment to any of the other Party's staff who have been associated

with the procurement and/or the contract management of the Services without that other Party's prior written consent.

## B10. MEETINGS AND REPORTS

- B10.1 The Contractor shall upon receipt of reasonable notice and during normal office hours attend all meetings arranged by the Authority for the discussion of matters connected with the performance of the Services.
- B10.2 Without prejudice to any other requirement in this Contract, the Contractor shall provide such reports on the performance of the Services as the Contract Manager may reasonably require.

## B11. SAFEGUARDING

- B11.1 For the purposes of this Clause B11, "**Reasonable Measures**" shall mean:

all reasonable endeavours expected to be taken by a professional and prudent supplier in the Supplier's industry to eliminate or minimise risk of actual, attempted or threatened exploitation, abuse and harassment (including Sexual Abuse, Sexual Exploitation and Sexual Harassment) and whether or not such conduct would amount to a criminal offence in the United Kingdom or an offence under the laws of the territory in which it takes place (together "**Serious Misconduct**") as is reasonable and proportionate under the circumstances. Such endeavours may include (but shall not be limited to):

- (a) Clear and detailed policies and guidance for Supplier Personnel, Supplier Providers and where appropriate, beneficiaries;
- (b) Developing, implementing and maintaining a safeguarding plan throughout the term (including monitoring);
- (c) Provision of regular training to Supplier Personnel, Supplier Providers and where appropriate, beneficiaries
- (d) Clear reporting lines and whistleblowing policies in place for Supplier Personnel, Supplier Providers and beneficiaries,
- (e) Maintaining detailed records of any allegations of Serious Misconduct and regular reporting to FCDO and the Appropriate Authorities (where relevant) of any such incidents;
- (f) Any other Good Industry Practice measures (including any innovative solutions),

- B11.2 The Supplier shall take all Reasonable Measures to prevent Serious Misconduct by the Supplier Personnel or any other persons engaged and controlled by it to perform any activities under this Agreement ("**Supplier Providers**") and shall have in place at all times robust procedures which enable the reporting by Supplier Personnel, Supplier Providers and beneficiaries of any such Serious Misconduct, illegal acts and/or failures by the Supplier or Supplier Personnel to investigate such reports.
- B11.3 The Supplier shall take all Reasonable Measures to ensure that the Supplier Personnel and Supplier Providers do not engage in sexual activity with any person under the age of 18, regardless of the local age of majority or age of consent or any mistaken belief held by the Supplier Personnel or Supplier Provider as to the age of the person. Furthermore, the Supplier shall ensure that the Supplier Personnel and Supplier Providers do not engage in 'transactional sex' which shall include but not be limited to the exchange of money, employment, goods, or services for sex and such reference to sex shall include sexual favours or any form of humiliating, degrading or exploitative behavior on the part of the Supplier Personnel and the Supplier Providers. For the avoidance of doubt, such 'transactional sex' shall be deemed to be Serious Misconduct in accordance with Clause B11.1.
- B11.4 The Supplier shall promptly report in writing any complaints, concerns and incidents regarding Serious Misconduct or any attempted or threatened Serious Misconduct by the Supplier Personnel and Supplier Providers to FCDO, including FCDO's Counter Fraud Section at [reportingconcerns@fcdo.gov.uk](mailto:reportingconcerns@fcdo.gov.uk) or +44 (0)1355 843747, and where necessary, the Appropriate Authorities.
- B11.5 The Supplier shall fully investigate and document all cases or potential cases of Serious Misconduct and shall take appropriate corrective action to reduce the risk and/or eliminate Serious Misconduct being committed by the Supplier Personnel and Supplier Providers (which may include disciplinary action, termination of contracts etc.), such investigations and actions to be reported to FCDO as soon as is reasonably practicable.
- B11.6 The Supplier shall not engage as Supplier Personnel or Supplier Provider for the purposes of the Services any person whose previous record or conduct known to the Supplier (or reasonably ought to be known by a diligent supplier which undertakes the appropriate checks) indicates that they are unsuitable to perform

the Services and/or where they represent an increased and unacceptable risk of committing Serious Misconduct.

B11.7 The Supplier shall comply with all applicable laws, legislation, codes of practice and government guidance in the UK and additionally, in the territories where the Services are being performed, relevant to safeguarding and protection of children and vulnerable adults, which the Supplier acknowledges may include vetting of the Supplier Personnel by the UK Disclosure and Barring Service in respect of any regulated activity performed by the Supplier Personnel (as defined by the Safeguarding Vulnerable Groups Act 2006 (as amended)) and/or vetting by a local equivalent service. Where FCDO reasonably believes that there is an increased risk to safeguarding in the performance of the Services, the Supplier shall comply with any reasonable request by FCDO for additional vetting to be undertaken.

B11.8 Failure by the Supplier to:

- 1) Put in place preventative measures to eliminate and/or reduce the risk of Serious Misconduct; or
- 2) Fully investigate allegations of Serious Misconduct; or
- 3) Immediate report any complaints to FCDO and where appropriate, the relevant authorities (including law enforcement)

shall be a material Default of this Contract and shall entitle FCDO to terminate this Contract with effect.

## C. PAYMENT AND CONTRACT PRICE

### C1. CONTRACT PRICE

C1.1 In consideration of the Contractor's performance of its obligations under the Contract, the Authority shall pay the charges in accordance with Condition C2 (Payment and VAT) and as set out in the Schedule of Prices and Rates.

C1.2 Where the parties have agreed in the Price Schedule that the Services will be provided on a fixed price basis, then the fixed price shall be paid according to the schedule of payments as detailed in the Price Schedule which may relate to the achievement of specific predefined milestones, dates or acceptance and shall be inclusive of all Contractor costs.

C1.3 From the date of the contract and every month thereafter, the Contractor shall provide a brief narrative report of activities undertaken under the Project and an assessment of the progress made against project outputs as set out Section 3 – Statement of Service Requirements. This assessment should provide evidence that the quality and timing criteria have been met.

### C2. PAYMENT AND VAT

C2.1 The Authority is committed to pay as soon as possible and shall pay all sums due to the Contractor within 30 days of receipt of a valid invoice, submitted monthly in arrears, unless otherwise agreed by the parties, to the invoicing address stipulated by the Authority in the Contract Award Letter.

C2.2 The Contractor shall ensure that each invoice contains all appropriate references and a detailed breakdown of the Services supplied and that it is supported by any other documentation reasonably required by the Authority to substantiate the invoice.

#### C2.2.1 NOT USED

C2.3 Where the Contractor enters into a sub-contract with a supplier or contractor for the purpose of performing its obligations under the Contract, it shall ensure that a provision is included in such a subcontract which requires payment to be made of all sums due by the Contractor to the sub-contractor as soon as possible and in any event not exceeding 30 days from the receipt of a valid invoice. The Authority reserves the right to ask for information about payment performance and will provide a facility for sub-contractors to report poor performance to the Authority.

C2.4 The Contractor shall add VAT to the Contract Price at the prevailing rate as applicable.

C2.5 The Contractor shall indemnify the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred which is levied, demanded or assessed on the Authority at any time in respect of the Contractor's failure to account for or to pay any VAT relating to payments made to the Contractor under the Contract. Any amounts due under this Condition C2.5 shall be paid by the Contractor to the Authority not less than 5 Working Days before the date upon which the tax or other liability is payable by the Authority.

C2.6 The Contractor shall not suspend the supply of the Services unless the Contractor is entitled to terminate the Contract under Condition H2.3 (Termination on Default) for failure to pay undisputed sums of money. Interest shall be payable by the Authority on the late payment of any undisputed sums of money properly invoiced in accordance with the Late Payment of Commercial Debts (Interest) Act 1998.

C2.7 If the Authority, acting in good faith, has a dispute in respect of any invoice, the Authority shall be entitled to withhold payment of the disputed amount, provided that it has notified the Contractor of the disputed amount and the nature of the dispute prior to the due date for payment of the invoice, and has paid any undisputed portion of the invoice to the Contractor. The parties will negotiate in good faith to resolve the dispute, and, failing resolution within five working days after receipt by the Contractor of the Authority's notification, the dispute will be referred to dispute resolution in accordance with Condition I2 (Dispute Resolution). In the event of such dispute, the Contractor shall continue to perform all its obligations under this Contract notwithstanding any withholding or reduction in payment by the Authority.

C2.8 The Authority may elect to pay for the Services by Government Procurement Card or such other method as the Parties may agree.

If the Authority elects to pay against an invoice, The Authority shall pay the Contractor within 30 days of receipt of an undisputed invoice by payment direct to the Contractors bank account as a credit transfer

### C3. RECOVERY OF SUMS DUE

C3.1 Any sum which is recoverable from or payable by the Contractor may be deducted from or reduced by any sum or sums then due or which may thereafter become due to the Contractor under or in respect of the Contract or any other contract with the Authority or any other government department or the Crown.

C3.2 Any overpayment by either Party, whether of the Contract Price or of VAT or otherwise, shall be a sum of money recoverable by the Party who made the overpayment from the Party in receipt of the overpayment.

C3.3 The Contractor shall make all payments due to the Authority without any deduction whether by way of set-off, counterclaim, discount, abatement or otherwise unless the Contractor has a valid court order requiring an amount equal to such deduction to be paid by the Authority to the Contractor.

C3.4 All payments due shall be made within a reasonable time unless otherwise specified in the Contract, in cleared funds, to such bank or building society account as the recipient Party may from time to time direct.

### C4. PRICE ADJUSTMENT

C4.1 The Contract Price shall, unless otherwise agreed in writing, be unchanged for a period of at least 5 years from the Commencement Date and shall then be subject to review, at one month's notice, by either party giving notice of such review to the other.

C4.2 In such review the Contract Price shall change by not more than the percentage change in the current (at the time of writing of the notice of the price review) Office of National Statistics' Consumer Prices Index (CPI) (or other such index specified in the Contract), from the same index 12 months earlier.

C4.3 Subsequent variations shall also be subject to one month's notice, as above, provided that each change is at least 12 months from the previous one. No price variation shall be retrospective.

C4.4 The Contractor may propose price reductions at any time.

## D. STATUTORY OBLIGATIONS AND REGULATIONS

### D1 PREVENTION OF CORRUPTION

D1.1 The Contractor shall not offer or give, or agree to give, to the Authority or any other public body or any person employed by or on behalf of the Authority or any other public body any gift or consideration of any kind as an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Contract or any other contract with the Authority or any other public body, or for showing or refraining from showing favour or disfavour to any person in relation to the Contract or any such contract.

D1.2 The Contractor warrants that it has not paid commission or agreed to pay commission to the Authority or any other public body or any person employed by or on behalf of the Authority or any other public body in connection with the Contract.

D1.3 If the Contractor, its Staff or anyone acting on the Contractor's behalf, engages in conduct prohibited by Conditions D1.1 or D1.2 or commits any offence under the Bribery Act 2010, the Authority may:

- (a) terminate the Contract and recover from the Contractor the amount of any loss suffered by the Authority resulting from the termination, including the cost reasonably incurred by the Authority of



making other arrangements for the supply of the Services and any additional expenditure incurred by the Authority throughout the remainder of the Contract Period; or

- (b) recover in full from the Contractor any other loss sustained by the Authority in consequence of any breach of those Conditions.

## D.2 PREVENTION OF FRAUD

- D2.1 The Contractor shall take all reasonable steps, in accordance with Good Industry Practice, to prevent Fraud by Staff and the Contractor (including its shareholders, members, directors) in connection with the receipt of monies from the Authority.
- D2.2 The Contractor shall notify the Authority immediately if it has reason to suspect that any Fraud has occurred or is occurring or is likely to occur.
- D2.3 If the Contractor or its Staff commits Fraud in relation to this or any other contract with the Crown (including the Authority) the Authority may:
  - (a) terminate the Contract and recover from the Contractor the amount of any loss suffered by the Authority resulting from the termination, including the cost reasonably incurred by the Authority of making other arrangements for the supply of the Services and any additional expenditure incurred by the Authority throughout the remainder of the Contract Period; or
  - (b) recover in full from the Contractor any other loss sustained by the Authority in consequence of any breach of this Condition.

## D.3 DISCRIMINATION

- D3.1 The Contractor shall not unlawfully discriminate either directly or indirectly on protected characteristics such as race, colour, ethnic or national origin, disability, sex or sexual orientation, religion or belief, or age and without prejudice to the generality of the foregoing the Contractor shall not unlawfully discriminate within the meaning and scope of the provisions of all relevant legislation including the Equality Act 2010 or other relevant or equivalent legislation, or any statutory modification or re-enactment thereof.
- D3.2 The Contractor shall adhere to the current relevant codes of practice or recommendations published by the Equality and Human Rights Commission. The Contractor shall take all reasonable steps to secure the observance of these provisions and codes of conduct by all contractors, employees or agents of the Contractor and all suppliers and Sub-contractors employed in the execution of this Contract.
- D3.3 The Contractor will comply with any request by the Authority to assist the Authority in meeting its obligations under the Equality Act 2010 and to allow the Authority to assess the Contractor's compliance with its obligations under the Equality Act 2010.
- D3.4 Where any investigation is concluded or proceedings are brought under the Equality Act 2010 which arise directly or indirectly out of any act or omission of the Contractor, its agents or sub contractors, or Staff, and where there is a finding against the Contractor in such investigation or proceedings, the Contractor will indemnify the Authority with respect to all costs, charges and expenses (including legal and administrative expenses) arising out of or in connection with any such investigation or proceedings and such other financial redress to cover any payment the Authority may have been ordered or required to pay to a third party.
- D3.5 Where in the reasonable opinion of the authority the Contractor has breached its obligations under Condition D3.1 or D3.2 (Discrimination) the Authority may terminate this Contract with immediate effect.

## D.4 THE CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

- D4.1 A person who is not a Party to the Contract shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of both Parties. This Condition does not affect any right or remedy of any person which exists or is available apart from the Contracts (Rights of Third Parties) Act 1999 and does not apply to the Crown.

## D.5 ENVIRONMENTAL REQUIREMENTS

- D5.1 The Contractor shall, when working on the Premises, perform its obligations under the Contract in accordance with the Authority's environmental policy, which is to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment.

- D5.2 All written work, including reports, delivered in connection with this Contract shall (unless otherwise specified) be produced on recycled paper containing 100% post consumer waste and used on both sides where appropriate. Paper used for printed publications must contain at least 75% recycled fibre paper in accordance with the UK government's timber procurement policy.
- D5.3 All timber or wood-derived products procured as part of this contract must originate from either legal and sustainable or FLEGT licensed or equivalent sources.
- D5.4 All goods purchased by the Contractor on behalf of the Authority (or which will become the property of the Authority) must comply with the relevant minimum environmental standards specified in the [Government Buying Standards](#) unless otherwise specified or agreed in writing.
- D.6 HEALTH AND SAFETY – NOT USED

#### D.7 THE TRANSFER OF UNDERTAKINGS (PROTECTION OF EMPLOYMENT) REGULATIONS 2006 (TUPE 2006)

##### Option A

- D7.1 The Contractor shall provide the Department, or any other person authorised by the Department who is to be invited to submit a tender in relation to the provision of similar Services, with such information (including any changes to and interpretations thereof) in connection with TUPE as the Department may require. The Contractor shall provide the information within 10 days of the Department's request.
- D7.2 During the 8 month period preceding the Expiry Date or any notice period, the Contractor shall not without the prior consent of the Department (which shall be in writing, but shall not be unreasonably withheld or delayed) move or deploy any Key Personnel away from the performance of the Services under this Contract.
- D7.3 Save where the Services comprise the provision of a consultancy service, during the 8 month period preceding the date of expiry set out in condition A2 (initial contract period) or any notice period, the Contractor shall not without the prior consent of the Authority (which shall be in writing, but shall not be unreasonable withheld or delayed):
- (a) materially amend the terms and conditions of employment of any employee whose work, wholly or mainly falls within the scope of this Contract; or
  - (b) materially increase the number of employees whose work (or any part of it) is work undertaken for the purposes of this Contract; or
- D7.4 The Contractor shall not knowingly do, or omit to do, anything which may adversely affect the orderly transfer of responsibility for provision of the Services.

#### E. PROTECTION OF INFORMATION

##### E1 DATA PROTECTION

- E1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor unless otherwise specified in Appendix G.2 to the Contract (Joint Controller Agreement). The only processing that the Contractor is authorised to do is listed in Appendix G.1 to the Contract (Processing, Personal Data and Data Subjects) by the Customer and may not be determined by the Contractor.
- E1.2 The Contractor shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.
- E1.3 The Contractor shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:
- (a) a systematic description of the envisaged processing operations and the purpose of the processing;
  - (b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
  - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and

- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

E1.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:

- (a) process that Personal Data only in accordance with Appendix G.1 to the Contract (Processing, Personal Data and Data Subjects), unless the Processor is required to do otherwise by Law. If it is so required the Contractor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
  - (i) nature of the data to be protected;
  - (ii) harm that might result from a Data Loss Event;
  - (iii) state of technological development; and
  - (iv) cost of implementing any measures;
- (c) ensure that:
  - (i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Appendix G.1 to the Contract (Processing, Personal Data and Data Subjects));
  - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
    - (A) are aware of and comply with the Processor's duties under this condition;
    - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
    - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
    - (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- (d) not transfer Personal Data outside of the UK or the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
  - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
  - (ii) the Data Subject has enforceable rights and effective legal remedies;
  - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
  - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
- (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

E1.5 Subject to Condition E1.6 (Data Protection), the Processor shall notify the Controller immediately if it:

- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
- (b) receives a request to rectify, block or erase any Personal Data;
- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

- (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
  - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;
- or
- (f) becomes aware of a Data Loss Event.

E1.6 The Processor's obligation to notify under Condition E1.5 (Data Protection) shall include the provision of further information to the Controller in phases, as details become available.

E1.7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Condition E1.5 (Data Protection) (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

- (a) the Controller with full details and copies of the complaint, communication or request;
- (b) such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
- (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- (d) assistance as requested by the Controller following any Data Loss Event;
- (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

E1.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this condition. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

- (a) the Controller determines that the processing is not occasional;
- (b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
- (c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

E1.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

E1.10 Each Party shall designate a data protection officer if required by the Data Protection Legislation.

E1.11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:

- (a) notify the Controller in writing of the intended Sub-processor and processing;
- (b) obtain the written consent of the Controller;
- (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Condition E1.4 (Data Protection) (such that they apply to the Sub-processor; and
- (d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

E1.12 The Processor shall remain fully liable for all acts or omissions of any Sub-processor.

E1.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this condition by replacing it with any applicable controller to processor standard conditions or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

E1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer may on not less than 30 Working Days' notice to the Contractor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

E1.15 Where the Parties include two or more Joint Controllers as identified in Appendix G.1 to the Contract (Processing, Personal Data and Data Subjects) in accordance with GDPR Article 26, those Parties shall

enter into a Joint Controller Agreement based on the terms outlined in Appendix G.2 to the Contract (Joint Controller Agreement) in replacement of Conditions 1.1-1.14 for the Personal Data under Joint Control.

E2 OFFICIAL SECRETS ACTS 1911, 1989, S182 OF THE FINANCE ACT 1989

E2.1 The Contractor shall comply with, and shall ensure that its Staff comply with, the provisions of:

- (a) the Official Secrets Acts 1911 to 1989; and
- (b) Section 182 of the Finance Act 1989.

E2.2 In the event that the Contractor or its Staff fail to comply with this Condition, the Authority reserves the right to terminate the Contract by giving notice in writing to the Contractor.

## E3 CONFIDENTIALITY

- E3.1 The parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, and specifically the information detailed in Appendix D "Commercially Sensitive information", the content of this Contract is not Confidential Information. The Authority shall be responsible for determining in its absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of the FOIA. Notwithstanding any other term of this Contract, the Contractor gives consent to the Authority to publish the Contract in its entirety, (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted) including from time to time agreed changes to the Contract, to the general public.
- E3.2 The Authority may consult with the Contractor to inform its decision regarding any exemptions to FOIA but the Authority shall have the final decision in its absolute discretion.
- E3.3 The Contractor shall assist and cooperate with the Authority to enable the Authority to publish this Agreement.
- E3.4 Condition E3.2 (Confidentiality) shall not apply to the extent that:
- E3.4.1 Such disclosure is a requirement of Law placed upon the party making the disclosure, including any requirements for disclosure under the FOIA, Code of Practice on Access to Government Information or the EIR, save that the Contractor shall not disclose any information relating to the Contract or the Authority's activities without the prior written consent of the Authority, which shall not be unreasonably withheld.
- E3.4.2 Such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;
- E3.4.3 Such information was obtained from a third party without obligation of confidentiality;
- E3.4.4 Such information was already in the public domain at the time of disclosure otherwise than by a breach of this Contract; or
- E3.4.5 It is independently developed without access to the other party's Confidential Information.
- E3.5 The Contractor may only disclose the Authority's Confidential Information to the persons it has employed or engaged who are directly involved in the provision of the Services and who need to know the information, and shall ensure that such persons are aware of and shall comply with these obligations as to confidentiality.
- E3.6 The Contractor shall not, and shall procure that the persons it has employed or engaged do not, use any of the Authority's Confidential Information received otherwise than for the purposes of this Contract.
- E3.7 At the written request of the Authority, the Contractor shall procure that those persons it has employed or engaged identified in the Authority's notice sign a confidentiality undertaking prior to commencing any work in accordance with this Contract.
- E3.8 Nothing in this Contract shall prevent the Authority from disclosing the Contractor's Confidential Information:
- E3.8.1 To any Crown Body or Overseas Governments, specifically those detailed in Annex 2 "Partners Across Government on the One HMG Overseas Platform" and any future Partners Across Government on the One HMG overseas platform as may be notified to the Contractor from time to time. All Crown Bodies receiving such Confidential Information shall be entitled to further disclose the Confidential Information to other Crown Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown Body. Disclosure is subject to the Authority's prior written notice and Contractor's prior written consent and on the proviso that the recipient of the information has undertaken, in writing, only to use it for the purposes of such review or examination and to comply with all the confidentiality provisions of this agreement;
- E3.8.2 To any consultant, contractor or other person engaged by the Authority or any person conducting a Gateway or other assurance review. Disclosure is subject to the Authority's prior written notice and Contractor's prior written consent and on the proviso that the recipient of the information has undertaken, in writing, only to use it for the purposes of such review or examination and to comply with all the confidentiality provisions of this agreement;
- E3.8.3 For the purpose of the examination and certification of the Authority's accounts. Disclosure is subject to the Authority's prior written notice and on the proviso that the recipient of the information has undertaken, in writing, only to use it for the purposes of such review or examination and to comply with all the confidentiality provisions of this agreement.; or
- E3.8.4 For any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources. Disclosure is subject to the Authority's

prior written notice and on the proviso that the recipient of the information has undertaken, in writing, only to use it for the purposes of such review or examination and to comply with all the confidentiality provisions of this agreement.

- E3.9 The Authority shall use all reasonable endeavours to ensure that any Crown Body, employee, third party or sub-contractor to whom the Contractor's Confidential Information is disclosed pursuant to Condition E3.8 (Confidentiality) is made aware of the Authority's obligations of confidentiality.
- E3.10 Nothing in this Condition E3 (Confidentiality) shall prevent either party from using any techniques, ideas or know-how gained during the performance of this Contract in the course of its normal business to the extent that this use does not result in a disclosure of the other party's Confidential Information or an infringement of Intellectual Property Rights.
- E3.11 NOT USED
- E3.12 The provisions under this Condition E3 (Confidentiality) are without prejudice to the application of the Official Secrets Acts 1911 to 1989 to any Confidential Information.
- E5 PUBLICITY, MEDIA AND OFFICIAL ENQUIRIES
- E5.1 Without prejudice to the Authority's obligations under the FOIA, the Contractor shall not make any press announcement or publicise the Contract or any part thereof in any way, except with the prior written consent of the Authority.
- E5.2 Both Parties shall take reasonable steps to ensure that their servants, employees, agents, sub-contractors, suppliers, professional advisors and consultants comply with Condition E5.1.
- E6 SECURITY
- E6.1 The Contractor shall take all measures necessary to comply with the provisions of any enactment relating to security which may be applicable to the Contractor in the performance of the Services.
- E6.2 The Contractor shall take all reasonable measures, by the display of notices or other appropriate means, to ensure that Staff have notice that all provisions referred to in Condition E6.1 (Security) will apply to them and will continue to apply to them, if so applicable, after the expiry or earlier termination of the Contract.
- E6.3 The Contractor shall co-operate with any investigation relating to security which is carried out by the Authority or by any person who is responsible to the Authority for security matters and when required by the Authority's Representative -
  - a) shall make any Staff identified by the Authority's Representative available to be interviewed by the Authority's Representative, or by a person who is responsible to the Authority for security matters, for the purposes of the investigation. Staff shall have the right to be accompanied by the Contractor's Representative and to be advised or represented by any other person whose attendance at the interview is acceptable to both the Authority's Representative and the Contractor's Representative; and
  - b) shall provide all documents, records or other material of any kind which may reasonably be required by the Authority or by a person who is responsible to the Authority for security matters, for the purposes of the investigation, so long as the provision of that material does not prevent the Contractor from performing the Services. The Authority shall have the right to retain any such material for use in connection with the investigation and, so far as possible, shall provide the Contractor with a copy of any material retained.
- E6.4 NOT USED
- E6.5 NOT USED
- E6.6 NOT USED
- E6.7 NOT USED
- E6.8 NOT USED
- E6.9 The Contractor shall, as an enduring obligation throughout the Contract Period, use the latest versions of anti-virus definitions available [from an industry accepted anti-virus software vendor] to check for and delete Malicious Software from both the Authority's and the contractor's ICT systems.
- E6.10 Notwithstanding Condition E6.9, if Malicious Software is found, the parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency

or loss or corruption of Authority Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency.

E6.11 Any cost arising out of the actions of the parties taken in compliance with the provisions of Condition E6.10 shall be borne by the parties as follows:

- a) by the Contractor where the Malicious Software originates from the Contractor Software, any third parties software used by the Contractor in providing the Services or the Authority Data (whilst the Authority Data was under the control of the Contractor); and
- b) by the Authority if the Malicious Software originates from the Authority Software or the Authority Data (whilst the Authority Data was under the control of the Authority).

## E7 INTELLECTUAL PROPERTY RIGHTS

E7.1 Intellectual Property Rights in the Services and any Deliverables under this Contract shall be vested in and owned absolutely by the Contractor (save that the Authority will retain ownership of any Authority Proprietary Materials which become imbedded in such Deliverables).

E7.2 For the duration of the contract and for a period of 12 months after the expiry or termination of the contract and the receipt by the Authority of the final set of deliverables from the Contractor, the Contractor will grant the Authority a non-exclusive, non-transferable, non-sublicensable, worldwide, royalty-free licence to use the Contractor's Intellectual Property Rights solely as necessary for the Authority to obtain the benefit of the Contractor's services, solely for its own business purposes and wholly in accordance with these conditions.

E7.3 The Contractor warrants, represents and undertakes that its provision of Services and Deliverables under this Contract will not infringe any Intellectual Property Rights of which a third party is the proprietor and that the Contractor is free to grant the license set out in condition E7.2 (Intellectual Property Rights). The Contractor agrees to indemnify and hold harmless the Authority against any and all liability, loss, damage, costs and expenses (including legal costs) which the Authority may incur or suffer as a result of any claim of alleged or actual infringement of a third party's Intellectual Property Rights by reason of either its or the Contractor's possession or use in any manner of any Deliverables or Services.

## E8 AUDIT

E8.1 The Contractor shall keep secure and maintain until six years after the final payment of all sums due under the Contract, or such other period as may be agreed between the Parties, full and accurate records of the Services, all expenditure reimbursed by the Authority and all payments made by the Authority.

E8.2 The Contractor shall grant to the Authority, or its authorised agents, such access to those records as they may reasonably require in order to check the Contractor's compliance with the Contract.

E8.3 For the purposes of the examination and certification of the Authority's accounts, or any examination under section 6(1) of the National Audit Act 1983 or annual re-enactment thereof as to the economy, efficiency and effectiveness with which the Authority has used its resources, the Comptroller and Auditor General may examine such documents as he may reasonably require which are owned, held or otherwise within the control of the Contractor and may require the Contractor to provide such oral or written explanations as he may reasonably require for those purposes. The Contractor shall give all reasonable assistance to the Comptroller and Auditor General for those purposes.

E8.4 Condition E8.3 (Right of Audit) applies only in respect of documents relating to the Contract and only for the purpose of the auditing of the Authority. It does not constitute an agreement under section 6(3)(d) of the National Audit Act 1983 such as to make the Contractor the subject of auditing under that Act.

E8.5 Except where an audit is imposed on the Authority by a Regulatory Body (in which case the Authority may carry out the audit required without prejudice to its other rights) the Authority may conduct an audit:

- a) to review the integrity, confidentiality and security of the Authority Data;
- b) to review the Contractor's compliance with the Data Protection Act 1998, the Freedom of Information Act 2000 in accordance with Condition E1 (Data Protection Act) and Condition E4 (Freedom of Information Act) and any other legislation applicable to the Services.

E8.6 Subject to the Authority's obligations of confidentiality, the Contractor shall on demand provide the Authority (and/or its agents or representatives) with all reasonable co-operation and assistance in relation to each audit, including:

- a) all information requested by the Authority within the permitted scope of the audit;



- b) reasonable access to any Sites controlled by the Contractor and to any equipment used (whether exclusively or non-exclusively) in the performance of the Services;
- c) access to the Contractor's system; and
- d) access to the Contractor's Staff.

## E9 AUTHORITY DATA

- E9.1 The Contractor shall not delete or remove any proprietary notices contained within or relating to the Authority Data.
- E9.2 The Contractor shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Contractor of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.
- E9.3 To the extent that Authority Data is held and/or processed by the Contractor, the Contractor shall supply that Authority Data to the Authority as requested by the Authority in the format specified in Section 4 - Statement of Service Requirements.
- E9.4 The Contractor shall take responsibility for preserving the integrity of Authority Data and preventing the corruption or loss of Authority Data.
- E9.5 The Contractor shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the Business Continuity and Disaster Recovery Plan at Appendix I. The Contractor shall ensure that such back-ups are available to the Authority at all times upon request and are delivered to the Authority at no less than monthly intervals.
- E9.6 The Contractor shall ensure that any system on which the Contractor holds any Authority Data, including back-up data, is a secure system that complies with The Security Policy.
- E9.7 If the Authority Data is corrupted, lost or sufficiently degraded as a result of the Contractor's Default so as to be unusable, the Authority may:
  - a) require the Contractor (at the Contractor's expense) to restore or procure the restoration of Authority Data in accordance with the Business Continuity and Disaster Recovery Plan at Appendix I and the Contractor shall do so as soon as practicable but not later than monthly; and/or
  - b) itself restore or procure the restoration of Authority Data, and shall be repaid by the Contractor any reasonable expenses incurred in doing so in accordance with the Business Continuity and Disaster Recovery Plan at Appendix I. If at any time the Contractor suspects or has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Contractor shall notify the Authority immediately and inform the Authority of the remedial action the Contractor proposes to take.

## E10 REMOVABLE MEDIA – NOT USED

## E11 TRANSPARENCY

- E11.1 The parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Contract is not Confidential Information. The Authority shall be responsible for determining in its absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of the FOIA.
- E11.2 Notwithstanding any other term of this Contract, the Contractor hereby gives his consent for the Authority to publish the Contract in its entirety, including from time to time agreed changes to the Agreement, to the general public.
- E11.3 The Authority may consult with the Contractor to inform its decision regarding any redactions but the Authority shall have the final decision in its absolute discretion.
- E11.4 The Contractor shall assist and cooperate with the Authority to enable the Authority to publish this Contract.

## F. CONTROL OF THE CONTRACT

### F1 TRANSFER AND SUB-CONTRACTING

- F1.1 Except where F1.4 and 5 applies, the Contractor shall not assign, sub-contract or in any other way dispose of the Contract or any part of it without prior Approval. Sub-contracting any part of the Contract shall not relieve the Contractor of any of its obligations or duties under the Contract.
- F1.2 The Contractor shall be responsible for the acts and omissions of its sub-contractors as though they are its own.
- F1.3 Where the Authority has consented to the placing of sub-contracts, copies of each sub-contract shall, at the request of the Authority, be sent by the Contractor to the Authority as soon as reasonably practicable.
- F1.4 Notwithstanding Condition F1.1, the Contractor may assign to a third party ("**the Assignee**") the right to receive payment of the Contract Price or any part thereof due to the Contractor under this Contract (including any interest which the Authority incurs under Condition C2.6). Any assignment under this Condition F1.4 shall be subject to:
- (a) reduction of any sums in respect of which the Authority exercises its right of recovery under Condition C3 (Recovery of Sums Due);
  - (b) all related rights of the Authority under the contract in relation to the recovery of sums due but unpaid; and
  - (c) the Authority receiving notification under both Conditions F1.5 and F1.6.
- F1.5 In the event that the Contractor assigns the right to receive the Contract Price under Condition F1.4, the Contractor or the Assignee shall notify the Authority in writing of the assignment and the date upon which the assignment becomes effective.
- F1.6 The Contractor shall ensure that the Assignee notifies the Authority of the Assignee's contact information and bank account details to which the Authority shall make payment.
- F1.7 The provisions of Condition C2 (Payment and VAT) shall continue to apply in all other respects after the assignment and shall not be amended without the approval of the Authority.
- F1.8 Subject to Condition F1.10, the Authority may assign novate or otherwise dispose of its rights and obligations under the Contract or any part thereof to:
- (a) any Contracting Authority; or
  - (b) any other body established by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Authority; or
  - (c) any private sector body which substantially performs the functions of the Authority, provided that any such assignment, novation or other disposal shall not increase the burden of the Contractor's obligations under the Contract.
- F1.9 Any change in the legal status of the Authority such that it ceases to be a Contracting Authority shall not, subject to Condition F1.8, affect the validity of the Contract. In such circumstances, the Contract shall bind and inure to the benefit of any successor body to the Authority.
- F1.10 If the rights and obligations under the Contract are assigned, novated or otherwise disposed of pursuant to Condition F1.6 to a body which is not a Contracting Authority or if there is a change in the legal status of the Authority such that it ceases to be a Contracting Authority (in the remainder of this Condition both such bodies being referred to as the "**Transferee**"):
- (a) the rights of termination of the Authority in Conditions H1 (Termination on change of control and insolvency) and H2 (Termination on Default) shall be available to the Contractor in the event of respectively, the bankruptcy or insolvency, or Default of the Transferee; and
  - (b) the Transferee shall only be able to assign, novate or otherwise dispose of its rights and obligations under the Contract or any part thereof with the prior consent in writing of the Contractor.
- F1.11 The Authority may disclose to any Transferee any Confidential Information of the Contractor which relates to the performance of the Contractor's obligations under the Contract. In such circumstances the Authority shall authorise the Transferee to use such Confidential Information only for purposes relating to the performance of the Contractor's obligations under the Contract and for no other purpose and shall take all reasonable steps to ensure that the Transferee gives a confidentiality undertaking in relation to such Confidential Information.
- F1.12 Each Party shall at its own cost and expense carry out, or use all reasonable endeavours to ensure the carrying out of, whatever further actions (including the execution of further documents) the other Party

reasonably requires from time to time for the purpose of giving that other party the full benefit of the provisions of the Contract.

F1.13 NOT USED

F1.14 NOT USED

F1.15 NOT USED

F1.16 NOT USED

F1.17 NOT USED

## F2 WAIVER

F2.1 The failure of either Party to insist upon strict performance of any provision of the Contract, or the failure of either Party to exercise, or any delay in exercising, any right or remedy shall not constitute a waiver of that right or remedy and shall not cause a diminution of the obligations established by the Contract.

F2.2 No waiver shall be effective unless it is expressly stated to be a waiver and communicated to the other Party in writing in accordance with Condition A5 (Notices).

F2.3 A waiver of any right or remedy arising from a breach of the Contract shall not constitute a waiver of any right or remedy arising from any other or subsequent breach of the Contract.

## F3 VARIATION

F3.1 Subject to the provisions of this Condition F3, the Authority may request a variation to the Specification provided that such variation does not amount to a material change to the Specification. Such a change is hereinafter called a "Variation".

F3.2 The Authority may request a Variation by notifying the Contractor in writing of the "Variation" and giving the Contractor sufficient information to assess the extent of the Variation and consider whether any change to the Contract Price is required in order to implement the Variation. The Authority shall specify a time limit within which the Contractor shall respond to the request for a Variation. Such time limits shall be reasonable having regard to the nature of the Variation. If the Contractor agrees with the proposed Variation it shall confirm the same in writing.

F3.3 In the event that the Contractor is unable to accept the Variation to the Specification or where the Parties are unable to agree a change to the Contract Price, the Authority may;

- (a) allow the Contractor to fulfil its obligations under the Contract without the variation to the Specification; or
- (b) terminate the Contract with immediate effect, except where the Contractor has already delivered all or part of the Services or where the Contractor can show evidence of substantial work being carried out to fulfil the requirements of the Specification; and in such case the Parties shall attempt to agree upon a resolution to the matter. Where a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution procedure detailed at Condition I2.

## F4 SEVERABILITY

F4.1 If any provision of the Contract is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision shall be severed and the remainder of the provisions of the Contract shall continue in full force and effect as if the Contract had been executed with the invalid, illegal or unenforceable provision eliminated.

## F5 REMEDIES IN THE EVENT OF INADEQUATE PERFORMANCE

F5.1 Where a complaint is received about the standard of Services or about the manner in which any Services have been supplied or work has been performed or about the materials or procedures used or about any other matter connected with the performance of the Contractor's obligations under the Contract, then the Authority shall notify the Contractor, and where considered appropriate by the Authority, investigate the complaint. The Authority may, in its sole discretion, uphold the complaint and take further action in accordance with clause H2 (Termination on Default) of the Contract.

F5.2 In the event that the Authority is of the reasonable opinion that there has been a material breach of the Contract by the Contractor, then the Authority may, without prejudice to its rights under clause H2 (Termination on Default), do any of the following:

- (a) without terminating the Contract, itself supply or procure the supply of all or part of the Services until such time as the Contractor shall have demonstrated to the reasonable satisfaction of the Authority

that the Contractor will once more be able to supply all or such part of the Services in accordance with the Contract;

- (b) without terminating the whole of the Contract, terminate the Contract in respect of part of the Services only (whereupon a corresponding reduction in the Contract Price shall be made) and thereafter itself supply or procure a third party to supply such part of the Services; and/or
- (c) terminate, in accordance with clause H2 (Termination on Default), the whole of the Contract.

F5.3 Without prejudice to its right under clause C3 (Recovery of Sums Due), the Authority may charge the Contractor for any costs reasonably incurred and any reasonable administration costs in respect of the supply of any part of the Services by the Authority or a third party to the extent that such costs exceed the payment which would otherwise have been payable to the Contractor for such part of the Services and provided that the Authority uses its reasonable endeavours to mitigate any additional expenditure in obtaining replacement Services.

F5.4 If the Contractor fails to supply any of the Services in accordance with the provisions of the Contract and such failure is capable of remedy, then the Authority shall instruct the Contractor to remedy the failure and the Contractor shall at its own cost and expense remedy such failure (and any damage resulting from such failure) within 10 Working Days or such other period of time as the Authority may direct.

F5.5 In the event that:

- a) the Contractor fails to comply with clause F5.4 above and the failure is materially adverse to the interests of the Authority or prevents the Authority from discharging a statutory duty; or
  - (b) the Contractor persistently fails to comply with clause F5.4 above,
- the Authority may terminate the Contract with immediate effect by notice in writing.

## F6 REMEDIES CUMULATIVE

F6.1 Except as otherwise expressly provided by the Contract, all remedies available to either Party for breach of the Contract are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.

## F7 MONITORING OF CONTRACT PERFORMANCE

F7.1 Prior to the Commencement Date the Authority shall agree in consultation with the Contractor the arrangements for the purpose of monitoring of performance by the Contractor of its obligations under this Contract, based on the requirements detailed in Section 4 - Statement of Service Requirements.

F7.2 These arrangements will include without limitation:

- i. random inspections;
- ii. regular meetings;
- iii. the regular delivery of written management reports;
- iv. adherence to KPIs to be reported in the regular meetings.

F7.3 All such arrangements will be carried out by the Contractor in a timely manner, as reasonably required by the Authority, and in line with Good Industry Practice.

F7.4 Failure to meet the KPIs specified in Section 4 - Statement of Services Requirement will entitle the Authority to claim from the Contractor the rebates as set out in Section 4 - Statement of Services Requirement.

## F8 ENTIRE AGREEMENT

F8.1 The Contract constitutes the entire agreement between the Parties in respect of the matters dealt with therein. The Contract supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral, except that this Condition shall not exclude liability in respect of any Fraud or fraudulent misrepresentation.

F8.2 If there is any conflict between the Sections and the Schedules and/or any appendices or other documents referred to in the Agreement, the following order or precedence shall apply:

Form of Contract	Section 1
Conditions of Contract	Section 2
Schedule of Prices and Rates	Section 4

## Statement of Service Requirements and KPIs      Section 3

Security requirement and plan      E9 AUTHORITY DATA and Appendix I Supplier  
Business Continuity and Disaster Recovery Plan

- F9. IMPROVING VISIBILITY OF SUBCONTRACT OPPORTUNITIES AVAILABLE TO SMES AND VCSES IN THE SUPPLY CHAIN – NOT USED
- F10. MANAGEMENT CHARGES AND INFORMATION – NOT USED
- F.11 FINANCIAL DISTRESS
- F11.1 The Contractor acknowledges and agrees that the financial stability and solvency of the Contractor and its key Sub-Contractors is critical to the successful delivery of the Services and that any deterioration or potential deterioration of their financial position may have an adverse effect on the performance of the Contract. The Contractor shall monitor its own financial standing and that of its key Sub-Contractors on a regular basis throughout the term using a Financial Monitoring Plan and shall report on this to the Authority.
- F11.2 The Financial Monitoring Plan shall be designed by the Contractor to ensure that the Authority has an early and clear warning indicator of any financial distress of the Contractor and key Sub-Contractors which may affect the Services; such design to be proportionate for the circumstances; taking into account the nature of the Services and the identity of the Contractors.
- F11.3 Except where the Authority has agreed otherwise, the Contractor shall within four (4) weeks of the Commencement Date, prepare and submit via the Project Officer for Approval by the Authority, a Financial Monitoring Plan which shall set out the Contractor's proposals for the monitoring and reporting of its financial stability, and the financial stability of its key Sub-Contractors to the Authority on a regular basis throughout the Term.
- F11.4 The Financial Monitoring Plan may include (but shall not be limited to):
- F11.4.1 A summary of the Contractor's and key Sub-Contractors' financial positions at the date of submission of the Financial Distress Plan and on a regular basis thereafter to the Authority (including credit ratings, financial ratios, details of current liabilities, value of marketable securities, cash in hand and bank, account receivables etc.);
- F11.4.2 An objective means of measuring the Contractor and key Sub-Contractor's financial standing on a regular basis throughout the Term against historical financial standing to show trend (including use of credit ratings, financial ratios and/or other financial indicators);
- F11.4.3 The Contractor's proposals for reporting financial standing to the Authority (including the template reporting forms which the Contractor intends to use);
- F11.4.4 The frequency of monitoring and reporting activity;
- F11.4.5 Provision of reporting lines for the supply chain to notify the Authority of incidents of non-payment of valid and undisputed invoices;
- F11.4.6 Any other provisions which in the reasonable opinion of the Contractor may be required by the Authority to assess current financial standing of the Contractor and key Sub-Contractors and which enable quick and easy assessment of any movement in financial standing.
- F11.5 The Contractor shall make any reasonable amendments to the Financial Monitoring Plan as may be requested by the Authority and shall resubmit it for Approval. If Approved by the Authority, the Contractor shall promptly implement the Financial Monitoring Plan throughout the Term.
- F11.6 In addition to its obligations under the Financial Monitoring Plan, the Contractor shall promptly notify the Authority in writing if any of the following "Financial Distress Events" occurs in respect of the Contractor or a key Sub-Contractor:
- F11.6.1 there is a material deterioration of its financial standing;
- F11.6.2 the appointment of an administrator or receiver;
- F11.6.3 late filing of statutory accounts with Companies House;
- F11.6.4 it issues a profits warning or other similar public announcement about a deterioration in its finances or prospects;

F11.6.5 it is being publicly investigated for improper financial accounting and reporting, fraud or any other financial impropriety;

F11.6.6 it commits a material breach of covenant to its lenders;

F11.6.7 a key Sub-Contractor not being paid any sums properly due under a specified invoice that is not subject to a genuine dispute;

F11.6.8 it is subject to any claims, litigation, investigations, actions or decisions in respect of financial indebtedness;

F11.7 In the event of a Financial Distress Event occurring, then the Contractor shall and shall procure that any affected key Sub-Contractor shall, as soon as reasonably practicable review the effect of the Financial Distress Event on the continued performance of the Services under this Contract and provide a report to the Authority. Where the Authority reasonably believes that the Financial Distress Event is likely to adversely impact on the performance of the Services, the Contractor shall submit to the Authority for Approval a Financial Distress Service Continuity Plan as soon as is reasonably practicable and shall provide any further financial information as the Authority may reasonably require to assess financial standing and risks.

F11.8 If the Authority acting reasonably considers that the Financial Distress Service Continuity Plan is insufficient to remedy the effects of the Financial Distress Event on the Service, then it may require the Contractor (and/or key Sub-Contractor) to redraft and resubmit an improved and updated plan or may require the issue to be escalated via the Dispute Resolution Procedure.

F11.9 If the Authority Approves the Financial Distress Service Continuity Plan, then the Contractor shall execute and continue to review the plan (with submissions to the Authority for Approval where it is updated).

F11.10 Where the Parties agree that the Financial Distress Event no longer adversely affects the delivery of the Services, the Contractor shall be relieved of its obligations in respect of the current Financial Distress Service Continuity Plan.

F11.11 the Authority shall be entitled to terminate this Contract for material Default if:

F11.11.1 The Contractor fails to notify the Authority of a Financial Distress Event in accordance with Clause F11.6;

F11.11.2 the Authority and the Contractor fail to agree a Financial Distress Service Continuity Plan or any updates to a plan within a reasonable timescale (taking into account the effects of the Financial Distress Event on the Services);

F11.11.3 The Contractor fails to comply with the terms of the Financial Distress Service Continuity Plan or any updates to the plan.

## G. LIABILITIES

### G1 LIABILITY, INDEMNITY AND INSURANCE

G1.1 Neither Party excludes or limits liability to the other Party for:

- (a) NOT USED
- (b) Fraud; or
- (c) Fraudulent misrepresentation; or
- (d) Any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982.
- (e) breach of Condition E3 (Confidentiality); or
- (f) NOT USED; or
- (g) breach of Condition E1 (Data Protection Act); or
- (h) NOT USED

G1.2 Subject to clauses G1.3 and G1.4, the Contractor shall indemnify the Authority and keep the Authority indemnified fully against all claims, proceedings, actions, damages, costs, expenses and any other liabilities which may arise out of, or in consequence of, the supply, or the late or purported supply, of the Services or the performance or non-performance by the Contractor of its obligations under the Contract or the presence of the Contractor or any Staff on the Premises, including in respect of financial loss arising from any services delivered or omitted to be delivered by the Contractor, or any other loss which is caused directly or indirectly by any act or omission of the Contractor.

- G1.3 The Contractor shall not be responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Authority or by breach by the Authority of its obligations under the Contract.
- G1.4 Subject always to clause G1.1, the liability of either Party for Defaults for (d), (e), or (g) shall be subject to the following financial limits:
- (a) the annual aggregate liability of either Party for Default resulting in direct loss of or damage to the property of the other under or in connection with the Contract shall in no event exceed twice the annual contract value;
  - (b) the annual aggregate liability under the Contract of either Party for Default (other than a Default governed by clauses E7.3 (Intellectual Property Rights) or G1.4(a)) shall in no event exceed twice the annual contract value unless otherwise agreed.
- G1.5 Subject always to clause G1.1, in no event shall either Party be liable to the other for any:
- (a) loss of profits, business, revenue or goodwill; and/or
  - (b) loss of savings (whether anticipated or otherwise); and/or
  - (c) indirect or consequential loss or damage.
- G1.6 The Contractor shall not exclude liability for additional operational, administrative costs and/or expenses or wasted expenditure resulting from the direct Default of the Contractor.
- G1.7 The Contractor shall effect and maintain with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Contractor, arising out of the Contractor's performance of its obligations under the Contract, including death or personal injury, loss of or damage to property or any other loss. Such policies shall include cover in respect of any financial loss arising from any advice given or omitted to be given by the Contractor. Such insurance shall be maintained for the duration of the Contract Period [and for a minimum of 6 (six) years following the expiration or earlier termination of the Contract].
- G1.8 The Contractor shall hold employer's liability insurance and public liability insurance in respect of Staff in accordance with any legal requirement from time to time in force.
- G1.9 The Contractor shall give the Authority, on request, copies of all insurance policies referred to in this clause or a broker's verification of insurance to demonstrate that the appropriate cover is in place, together with receipts or other evidence of payment of the latest premiums due under those policies.
- G1.10 If, for whatever reason, the Contractor fails to give effect to and maintain the insurances required by the provisions of the Contract the Authority may make alternative arrangements to protect its interests and may recover the costs of such arrangements from the Contractor.
- G1.11 The provisions of any insurance or the amount of cover shall not relieve the Contractor of any liabilities under the Contract. It shall be the responsibility of the Contractor to determine the amount of insurance cover that will be adequate to enable the Contractor to satisfy any liability referred to in clause G1.2.

## G2 PROFESSIONAL INDEMNITY

- G2.1 The Contractor shall effect and maintain appropriate professional indemnity insurance cover during the Contract Period and shall ensure that all agents, professional consultants and sub-contractors involved in the supply of the Services do the same. To comply with its obligations under this Condition and as a minimum, the Contractor shall ensure professional indemnity insurance held by the Contractor and by any agent, sub-contractor or consultant involved in the supply of the Services has a limit of indemnity of not less than Five Million pounds (£5,000,000) for each individual claim [or such other limit as the Authority may reasonably require (and as required by law) from time to time]. Such insurance shall be maintained for a minimum of 6 (six) years following the expiration or earlier termination of the Contract.

## G3 WARRANTIES AND REPRESENTATIONS

- G3.1 The Contractor warrants and represents that:
- (a) it has full capacity and authority and all necessary consents (including where its procedures so require, the consent of its parent company) to enter into and perform its obligations under the Contract and that the Contract is executed by a duly authorised representative of the Contractor;
  - (b) in entering the Contract it has not committed any Fraud;
  - (c) as at the Commencement Date, all information contained in the Tender remains true, accurate and not misleading, save as may have been specifically disclosed in writing to the Authority prior

to execution of the Contract; The Contractor warrants that the Services which it provides under the Contract correspond to the Authority's requirements and is consistent with the standards that are referred to in Condition 3.1 and any other standards which may be implied by statute or common law that apply to this Contract may not be excluded.

- (d) no claim is being asserted and no litigation, arbitration or administrative proceeding is presently in progress or, to the best of its knowledge and belief, pending or threatened against it or any of its assets which will or might have a material adverse effect on its ability to perform its obligations under the Contract;
- (e) it is not subject to any contractual obligation, compliance with which is likely to have a material adverse effect on its ability to perform its obligations under the Contract;
- (f) no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Contractor or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Contractor's assets or revenue;
- (g) it owns, has obtained or is able to obtain, valid licences for all Intellectual Property Rights that are necessary for the performance of its obligations under the Contract;
- (h) it has and will continue to hold all necessary (if any) regulatory approvals from the Regulatory Bodies necessary to perform the Contractor's obligations under this Contract;
- (i) in the three 3 years prior to the date of the Contract:
  - (i) it has conducted all financial accounting and reporting activities in compliance in all material respects with the generally accepted accounting principles that apply to it in any country where it files accounts;
  - (ii) it has been in full compliance with all applicable securities and tax laws and regulations in the jurisdiction in which it is established; and
  - (iii) it has not done or omitted to do anything which could have a material adverse effect on its assets, financial condition or position as an ongoing business concern or its ability to fulfil its obligations under the Contract.
- (j) in performing its obligations under this Contract, all software used by or on behalf of the Contractor will:
  - i. be currently supported versions of that software; and
  - ii. perform in all material respects in accordance with its specification.
- k) NOT USED
- L) NOT USED

## H. DEFAULT, DISRUPTION AND TERMINATION

### H1 TERMINATION ON INSOLVENCY AND CHANGE OF CONTROL

H1.1 The Authority may terminate the Contract with immediate effect by notice in writing where the Contractor is a company and in respect of the Contractor:

- (a) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or
- (b) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or
- (c) a petition is presented for its winding up (which is not dismissed within 14 days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or
- (d) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or
- (e) an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or
- (f) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or



- (g) being a “small company” within the meaning of section 247(3) of the Companies Act 1985, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or
- (h) any event similar to those listed in H1.1(a)-(g) occurs under the law of any other jurisdiction.
- (i) an application for an interim order is made pursuant to sections 252-253 of the Insolvency Act 1986 or a proposal is made for any composition scheme or arrangement with, or

H1.2 The Authority may terminate the Contract with immediate effect by notice in writing where the Contractor is an individual and:

- (a) an application for an interim order is made pursuant to sections 252-253 of the Insolvency Act 1986 or a proposal is made for any composition scheme or arrangement with, or assignment for the benefit of, the Contractor’s creditors; or
- (b) a petition is presented and not dismissed within 14 days or order made for the Contractor’s bankruptcy; or
- (c) a receiver, or similar officer is appointed over the whole or any part of the Contractor’s assets or a person becomes entitled to appoint a receiver, or similar officer over the whole or any part of his assets; or
- (d) the Contractor is unable to pay his debts or has no reasonable prospect of doing so, in either case within the meaning of section 268 of the Insolvency Act 1986; or
- (e) a creditor or encumbrancer 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 the Contractor’s assets and such attachment or process is not discharged within 14 days; or
- (f) he dies or is adjudged incapable of managing his affairs within the meaning of Part VII of the Mental Capacity Act 2005; or
- (g) he suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of his business.

H1.3 The Contractor shall seek the prior Approval of the Authority to any change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988 (“**change of control**”), such approval not to be unreasonably withheld. Where an Approval has not been granted prior to the change of control the Authority may terminate the Contract by notice in writing with immediate effect within six months of:

- (a) being notified that a change of control has occurred; or
- (b) where no notification has been made, the date that the Authority becomes aware of the change of control.

## H2 TERMINATION ON DEFAULT

H2.1 The Authority may terminate the Contract by written notice to the Contractor with immediate effect if the Contractor commits a Default and if:

- (a) the Contractor has not remedied the Default to the satisfaction of the Authority within 25 Working Days, or such other period as may be specified by the Authority, after issue of a written notice specifying the Default and requesting it to be remedied; or
- (b) the Default is not, in the opinion of the Authority, capable of remedy; or
- (c) the Default is a material breach of the Contract.

H2.2 In the event that through any Default of the Contractor, data transmitted or processed in connection with the Contract is either lost or sufficiently degraded as to be unusable, the Contractor shall be liable for the cost of reconstitution of that data and shall reimburse the Authority in respect of any charge levied for its transmission and any other costs charged in connection with such Default.

H2.3 If the Authority fails to pay the Contractor undisputed sums of money when due, the Contractor shall notify the Authority in writing of such failure to pay. If the Authority fails to pay such undisputed sums within 90 Working Days of the date of such written notice, the Contractor may terminate the Contract in writing with immediate effect, save that such right of termination shall not apply where the failure to pay is due to the Authority exercising its rights under clause C3.1 (Recovery of Sums Due).

H2.4 The Authority reserves the right to terminate the Contract should the Contractor be found to be in breach of any aspect of the law that would, in the opinion of the Authority, bring the Authority into disrepute,

including but not limited to, relevant aspects shown in Regulation 57 of Public Contract Regulations 2015 (as amended) relating to rejection criteria.

## H2.5 NOT USED

### H3 BREAK

- H3.1 The Authority shall have the right to terminate the Contract after the first anniversary of the Contract signing by giving 12 Months' written notice to the Contractor. The Authority shall have the right to terminate the Contract after the second anniversary of the Contract signing by giving 6 Months' written notice to the Contractor.

### H4 CONSEQUENCES OF EXPIRY OR TERMINATION

- H4.1 Where the Authority terminates the Contract under clause H2 (Termination on Default) and then makes other arrangements for the supply of Services, the Authority may recover from the Contractor the cost reasonably incurred of making those other arrangements and any additional expenditure incurred by the Authority throughout the remainder of the Contract Period. The Authority shall take all reasonable steps to mitigate such additional expenditure. Where the Contract is terminated under clause H2 (Termination on Default), no further payments shall be payable by the Authority to the Contractor (for Services supplied by the Contractor prior to termination and in accordance with the Contract but where the payment has yet to be made by the Authority), until the Authority has established the final cost of making the other arrangements envisaged under this clause.

- H4.2 Subject to clause G1, where the Authority terminates the Contract under clause H3 (Break), the Authority shall indemnify the Contractor against any commitments, liabilities or expenditure which represent an unavoidable direct loss to the Contractor by reason of the termination of the Contract, provided that the Contractor takes all reasonable steps to mitigate such loss. Where the Contractor holds insurance, the Authority shall only indemnify the Contractor for those unavoidable direct costs that are not covered by the insurance available. The Contractor shall submit a fully itemised and costed list of unavoidable direct loss which it is seeking to recover from the Authority, with supporting evidence, of losses reasonably and actually incurred by the Contractor as a result of termination under clause H3 (Break).

- H4.3 The Authority shall not be liable under clause H4.2 to pay any sum which:

- (a) was claimable under insurance held by the Contractor, and the Contractor has failed to make a claim on its insurance, or has failed to make a claim in accordance with the procedural requirements of the insurance policy;
- (b) when added to any sums paid or due to the Contractor under the Contract, exceeds the total sum that would have been payable to the Contractor if the Contract had not been terminated prior to the expiry of the Contract Period; or
- (c) is a claim by the Contractor for loss of profit, due to early termination of the Contract.

- H4.4 Save as otherwise expressly provided in the Contract:

- (a) termination or expiry of the Contract shall be without prejudice to any rights, remedies or obligations accrued under the Contract prior to termination or expiration and nothing in the Contract shall prejudice the right of either Party to recover any amount outstanding at such termination or expiry; and
- (b) termination of the Contract shall not affect the continuing rights, remedies or obligations of the Authority or the Contractor under clauses C2 (Payment and VAT), C3 (Recovery of Sums Due), D1 (Prevention of Corruption), E1 (Data Protection Act), E2 (Official Secrets Acts 1911 to 1989, Section 182 of the Finance Act 1989), E3 (Confidential Information), E4 (Freedom of Information), E7 (Intellectual Property Rights), E8 (Audit), F6 Remedies Cumulative), G1 (Liability, Indemnity and Insurance), G2 (Professional Indemnity), H4 (Consequences of Termination), H6 (Recovery upon Expiry or Termination) and I1 (Governing Law and Jurisdiction).

### H5 DISRUPTION

- H5.1 The Contractor shall take reasonable care to ensure that in the performance of its obligations under the Contract it does not disrupt the operations of the Authority, its employees or any other contractor employed by the Authority.
- H5.2 The Contractor shall immediately inform the Authority of any actual or potential industrial action, whether such action be by their own employees or others, which affects or might affect its ability at any time to perform its obligations under the Contract.

- H5.3 In the event of industrial action by the Staff, the Contractor shall seek Approval to its proposals to continue to perform its obligations under the Contract.
- H5.4 If the Contractor's proposals referred to in Condition H5.3 are considered insufficient or unacceptable by the Authority acting reasonably, then the Contract may be terminated with immediate effect by the Authority by notice in writing.
- H5.5 If the Contractor is temporarily unable to fulfil the requirements of the Contract owing to disruption of normal business of the Authority, the Contractor may request a reasonable allowance of time and in addition, the Authority will reimburse any additional expense reasonably incurred by the Contractor as a direct result of such disruption.
- H6 RECOVERY UPON TERMINATION
- H6.1 On the termination of the Contract for any reason, the Contractor shall:
- (a) immediately return to the Authority all Confidential Information, Personal Data and IP Materials in its possession or in the possession or under the control of any permitted suppliers or sub-contractors, which was obtained or produced in the course of providing the Services;
  - (b) immediately deliver to the Authority all Property (including materials, documents, information and access keys) provided to the Contractor under clause B8. Such property shall be handed back in good working order (allowance shall be made for reasonable wear and tear);
  - (c) assist and co-operate with the Authority to ensure an orderly transition of the provision of the Services to the Replacement Contractor and/or the completion of any work in progress.
  - (d) promptly provide all information concerning the provision of the Services which may reasonably be requested by the Authority for the purposes of adequately understanding the manner in which the Services have been provided or for the purpose of allowing the Authority or the Replacement Contractor to conduct due diligence.
- H6.2 If the Contractor fails to comply with clause H6.1 (a) and (b), the Authority may recover possession thereof and the Contractor grants a licence to the Authority or its appointed agents to enter (for the purposes of such recovery) any premises of the Contractor or its permitted suppliers or sub-contractors where any such items may be held.
- H6.3 Where the end of the Contract Period arises due to the Contractor's Default, the Contractor shall provide all assistance under clause H6(c) and (d) free of charge. Otherwise, the Authority shall pay the Contractor's reasonable costs of providing the assistance and the Contractor shall take all reasonable steps to mitigate such costs.
- H7 FORCE MAJEURE
- H7.1 For the purposes of this Contract the expression "**Force Majeure**" shall mean any cause outside the reasonable control of either Party affecting its performance of its obligations under this Agreement arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including acts of God, riots, war or armed conflict, acts of terrorism, acts of government, local government or regulatory bodies, fire, flood, storm or earthquake, or disaster but excluding any industrial dispute relating to the Contractor or the Contractor Personnel or any other failure in the Contractor's or a Sub-contractor's supply chain;
- H7.2 Neither Party shall be liable to the other Party for any delay in performing, or failure to perform, its obligations under the Contract (other than a payment of money) to the extent that such delay or failure is a result of Force Majeure. Notwithstanding the foregoing, each Party shall use all reasonable endeavours to continue to perform its obligations under the Contract for the duration of such Force Majeure. However, if such Force Majeure prevents either Party from performing its material obligations under the Contract for a period in excess of 6 Months, either Party may terminate the Contract with immediate effect by notice in writing.
- H7.3 Any failure or delay by the Contractor in performing its obligations under the Contract which results from any failure or delay by an agent, sub-contractor or Supplier shall be regarded as due to Force Majeure only if that agent, sub-contractor or supplier is itself impeded by Force Majeure from complying with an obligation to the Contractor.
- H7.4 If either Party becomes aware of Force Majeure which gives rise to, or is likely to give rise to, any failure or delay on its part as described in Condition H7.1 it shall immediately notify the other by the most expeditious method then available and shall inform the other of the period for which it is estimated that such failure or delay shall continue.

## H8 EXIT MANAGEMENT

- H8.1 On reasonable notice at any point during the Term, the Contractor shall provide to the Authority and/or its potential Replacement Contractors (subject to the potential Replacement Contractors entering into reasonable written confidentiality undertakings), the following material and information in order to facilitate the preparation by the Authority of any invitation to tender and/or to facilitate any potential Replacement Contractors undertaking due diligence:
- H8.1.1 details of the Service(s);
  - H8.1.2 a copy of the Register, updated by the Contractor up to the date of delivery of such Registers;
  - H8.1.3 an inventory of the Authority Data in the Contractor's possession or control;
  - H8.1.4 details of any key terms of any third party contracts and licences, particularly as regards charges, termination, assignment and novation;
  - H8.1.5 a list of on-going and/or threatened disputes in relation to the provision of the Services;
  - H8.1.6 all information relating to Transferring Contractor Employees or those who may be Transferring Contractor Employees' required to be provided by the Contractor under any Call-Off Contract pursuant to this Framework Agreement, such information to include the Staffing Information as defined in Schedule 2 (Staff Transfer); and
  - H8.1.7 such other material and information as the Authority shall reasonably require;  
(together, the "**Exit Information**").
- H8.2 The Contractor acknowledges that the Authority may disclose the Contractor's Confidential Information to an actual or prospective Replacement Contractor or any third party whom the Authority is considering engaging to the extent that such disclosure is necessary in connection with such engagement (except that the Authority may not disclose any Contractor's Confidential Information which is information relating to the Contractor's or its Sub-Contractors' prices or costs).
- H8.3 if the Exit Information materially changes from the Exit Information previously provided and it could reasonably adversely affect:
- H8.3.1 the provision of the Services; and/or
  - H8.3.2 the delivery of the exit services/exit plan; and/or
  - H8.3.3 any re-tender exercise by the Authority,
- then the Contractor shall notify the Authority within a reasonable period of time and consult and shall consult with the Authority regarding such proposed material changes and provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and in any event within ten (10) Working Days of a request in writing from the Authority.
- H8.4 The Exit Information shall be accurate and complete in all material respects and the level of detail to be provided by the Contractor shall be such as would be reasonably necessary to enable a third party to:
- H8.4.1 prepare an informed offer for those Services; and
  - H8.4.2 not be disadvantaged in any subsequent procurement process compared to the Contractor (if the Contractor is invited to participate).
- H8.5 The Contractor shall, within three (3) months after the Commencement Date, deliver to the Authority an Exit Plan which:
- H8.5.1 sets out the Contractor's proposed methodology for achieving an orderly transition of the Services from the Contractor to the Authority and/or its Replacement Contractor on the expiry or termination of a Call-Off Contract;
  - H8.5.2 complies with the requirements set out in Clause 16.7 below;
  - H8.5.3 is otherwise reasonably satisfactory to the Authority.
- H8.6 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- H8.7 Unless otherwise specified by the Authority, the Exit Plan shall set out, as a minimum:
- H8.7.1 how the Exit Information is obtained;

- H8.7.2 the management structure to be employed during both transfer and cessation of the Services;
- H8.7.3 the management structure to be employed whilst carrying out the activities to be performed by the Contractor as identified in the Exit Plan;
- H8.7.4 a detailed description of both the transfer and cessation processes, including a timetable;
- H8.7.5 how the Services will transfer to the Replacement Contractor and/or the Authority, including details of the processes, documentation, data transfer, systems migration, security and the segregation of the Authority's technology components from any technology components operated by the Contractor or its Sub-Contractors (where applicable);
- H8.7.6 details of contracts (if any) which will be available for transfer to the Authority and/or the Replacement Contractor upon the Expiry Date together with any reasonable costs required to effect such transfer (and the Contractor agrees that all assets and contracts used by the Contractor in connection with the provision of the Services will be available for such transfer);
- H8.7.7 proposals for the training of key personnel of the Replacement Contractor in connection with the continuation of the provision of the Services following the Expiry Date charged at rates agreed between the Parties at that time;
- H8.7.8 proposals for providing the Authority or a Replacement Contractor copies of all documentation:
  - (a) used in the provision of the Services and necessarily required for the continued use of the Replacement Services, in which the Intellectual Property Rights are owned by the Contractor; and
  - (b) relating to the use and operation of the Services;
- H8.7.9 proposals for the assignment or novation of the provision of all services, leases, maintenance agreements and support agreements utilised by the Contractor in connection with the performance of the supply of the Services;
- H8.7.10 proposals for the identification and return of all Equipment in the possession of and/or control of the Contractor or any third party (including any Sub-Contractor);
- H8.7.11 proposals for the disposal of any redundant Services and materials;
- H8.7.12 procedures to:
  - (a) deal with requests made by the Authority and/or a Replacement Contractor for Staffing Information pursuant to Schedule 2 (Staff Transfer);
  - (b) determine which Contractor Personnel are or are likely to become Transferring Contractor Employees; and
  - (c) identify or develop any measures for the purpose of the Employment Regulations envisaged in respect of Transferring Contractor Employees;
- H8.7.13 how each of the issues set out in this Clause 16 will be addressed to facilitate the transition of the Services from the Contractor to the Replacement Contractor and/or the Authority with the aim of ensuring that there is no disruption to or degradation of the Services;
- H8.7.14 proposals for the supply of any other information or assistance reasonably required by the Authority or a Replacement Contractor in order to effect an orderly handover of the provision of the Services.

## I. DISPUTES AND LAW

### I1 GOVERNING LAW AND JURISDICTION

- I1.1 Subject to the provisions of Condition I2, this Contract will be governed by and construed in accordance with English law and the Contractor hereby irrevocably submits to the jurisdiction of the English courts. The submission to such jurisdiction will not (and will not be construed so as to) limit the right of the Authority to take proceedings against the Contractor in any other court of competent jurisdiction, nor will the taking of proceedings by the Authority in any one or more jurisdictions preclude the taking of proceedings by the Authority in any other jurisdiction, whether concurrently or not.

### I2 DISPUTE RESOLUTION

- I2.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Contract by use of the following escalation procedure:

	<u>Authority</u>	<u>Contractor</u>
Level 1	[REDACTED]	[REDACTED]
Level 2	[REDACTED]	[REDACTED]

- I2.2 If the dispute cannot be resolved by the Parties pursuant to Condition I2.1 (Dispute Resolution), the dispute may, by agreement between the Parties, be referred to mediation pursuant to Condition I2.4 (Dispute Resolution).
- I2.3 The performance of the Services shall not cease or be delayed by the reference of a dispute to mediation pursuant to Condition I2.2 (Dispute Resolution).
- I2.4 The procedure for mediation and consequential provisions relating to mediation are as follows:
- a) If the dispute or difference is not resolved pursuant to the escalation procedure set out above, either Party may (within fourteen (14) days of the last meeting pursuant to the escalation procedure), before resorting to litigation, propose to the other in writing that the dispute be settled by mediation in accordance with the Centre for Effective Dispute Resolution (“CEDR”) Model Mediation Procedure (the “Model Procedure”).
  - b) To initiate mediation, a Party must give notice in writing (an “ADR Notice”) to the other Party requesting mediation in accordance with the Model Procedure. A copy of the ADR Notice should be sent to CEDR.
  - c) If there is any point on the conduct of the mediation (including as to the nomination of the mediator) upon which the Parties cannot agree within fourteen (14) days from the date of the ADR Notice, CEDR will, at the request of any Party, decide that point for the Parties, having consulted with them.
  - d) Mediation will commence no later than twenty-eight (28) days after the date of the ADR Notice.

#### J. FRAMEWORK PROVISIONS – NOT USED

#### K CATEGORY SPECIFIC CONDITIONS – NOT USED

##### K1 COMMENCEMENT OF FULL OPERATIONS – NOT USED

##### K2 CO-ORDINATION – NOT USED

##### K3 RESPONSIBILITY FOR EQUIPMENT – NOT USED

##### K4 TITLE AND RISK – NOT USED

##### K5 ACCEPTANCE – NOT USED

##### K6. FLEXIBLE OPERATIONS – NOT USED



**VARIATION TO CONTRACT FORM****Appendix A***See Condition F3***[To be completed according to specific contract and where relevant]**

CONTRACT NUMBER: Project\_9629 / ITT\_5816  
CONTRACT TITLE: Hardship and Cost of Living Data Processing & Provision  
VARIATION NUMBER: **[insert]**

BETWEEN The Secretary of State for Foreign and Commonwealth Affairs (hereinafter called 'the Authority' and ECA International (hereinafter called the Contractor')

1. The Contract is varied as follows:  
In consideration of **[insert]** the Parties agree to **[insert]**
2. Words and expressions in this Variation shall have the meanings given to them in the Contract.
3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

SIGNED by the Parties in duplicate:

For the Authority

By:

For the Contractor

By:

Full Name:

Title:

Date:

Full Name:

Title:

Date:

*SIGNED by the Parties in duplicate*



**CONFIDENTIALITY UNDERTAKING****Appendix B***See Condition E3.5*

(To be signed by persons employed in providing the services before being given access to Government information).

This Confidentiality Undertaking is made as a Deed by me, [insert full name] to the Secretary of State for Foreign, Commonwealth and Development Affairs (the "FCDO") in connection with a contract between ECA International and the FCDO for the provision of Hardship and Cost of Living Data Processing & Provision.

I am employed by ECA International. I have been informed that I may be required to work for my employer in providing services to the Secretary of State for Foreign, Commonwealth and Development Affairs.

I understand that information in the possession of the FCDO or obtained from the FCDO must be treated as confidential.

I hereby give a formal undertaking, as a solemn promise to my employer and to the FCDO, that:

1. I will not communicate any of that information, or any other knowledge I acquire about the FCDO in the course of my work, to anyone who is not authorised to receive it in connection with that work; and
2. I will not make use of any of that information or knowledge for any purpose apart from that work;

I acknowledge that this applies to all information that is not already a matter of public knowledge and that it applies to both written and oral information.

I also acknowledge that this undertaking will continue to apply at all times in the future, even when the work has finished and when I have left my employment.

I have also been informed that I will be bound by the provisions of the Official Secrets Acts 1911 to 1989. I am aware that under those provisions it is a criminal offence to disclose information that has been given to me or my employer by the FCDO. I am aware that serious consequences (including criminal sanctions) may follow any breach of those provisions.

EXECUTED AS A DEED by:

Contract Reference:

Surname:

Forenames:

Date of Signature:

In the presence of (a) (Witness)

In the presence of (b) (Witness)

Contractor's Name:

**KEY STAFF** for the provision of Hardship and Cost of Living Data Processing & Provision

## Appendix C

*See Condition B4*

[illegible]

**COMMERCIALLY SENSITIVE INFORMATION****Appendix D**

*See Condition E4.7*

Note: following condition extracted from 1.1

Note suitability of this Clause - "Commercially Sensitive Information" means the subset of Confidential Information listed in Appendix D comprised of information:

- (a) which is provided by the Contractor to the Authority in confidence for the period set out in that schedule; and/or
- (b) that constitutes a trade secret.

1. Contractor Schedule of Prices and Rates;
2. Contractor responses to Technical Evaluation Questions;
3. Data provided by the Contractor;
4. Methodology used by the Contractor.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

**SCHEDULE OF PROCESSING, PERSONAL DATA AND DATA SUBJECTS****Appendix G.1**

This Schedule shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are: Office of the Data Protection Officer, [REDACTED]
2. The contact details of the Processor's Data Protection Officer are: Chief Information Security Officer, [REDACTED]
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor in accordance with Condition E1.1.
Subject matter of the processing	Data which is to be processed in the provision of Hardship location scores, Cost of Living Allowance (COLA) rates, and associated services.
Duration of the processing	Processing of Personal Data will only be completed in accordance with Condition A2.1 and the timeframes stated therein. There is to be no further processing of Personal Data by the Contractor beyond expiry of this contract.
Nature and purposes of the processing	The Supplier will collect and process Personal Data for the purposes of providing Hardship location scores, Cost of Living Allowance (COLA) rates, and associated services. These services support the calculation of the Hardship element of Diplomatic Service Allowance (DSA) and Cost of Living Allowance (COLA) that the FCDO provides to its staff serving overseas.
Type of Personal Data being Processed	Personal Data collected and processed by the Supplier is to be limited to the following: <ul style="list-style-type: none"> <li>• Name (as required);</li> <li>• Work-email address (as required);</li> <li>• Mobile number (as required).</li> </ul>
Categories of Data Subject	Personal data will be collected and processed for current employees.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Incoming FCDO questionnaire responses are delivered into a dedicated mailbox that is not subject to usual / standard data retention rules to ensure prompt, permanent deletion at the end of the data's useful life. No personal data is saved on the questionnaire itself (no names etc.). A separate mailbox is also used for responses to the FCDO assignees, where necessary to confirm receipt of a response, for the same reasons.

**SUPPLIER CODE OF CONDUCT****Appendix H****FCDO SUPPLIER CODE OF CONDUCT****1. What we expect from our Suppliers**

- 1.1 Version 2 of the [Government Supplier Code of Conduct](#) ("the Code") sets out the standards and behaviours expected of suppliers who work with government.
- 1.2 The FCDO (henceforth known as "the Authority") expects its Suppliers and its Suppliers' Subcontractors to meet the standards set out in the Code. In addition, The FCDO expects its suppliers and its suppliers' subcontractors to comply with the standards set out in this Schedule.
- 1.3 The Supplier acknowledges that the Authority may have additional requirements in relation to corporate social responsibility. The Supplier and the Suppliers' Subcontractors shall comply with such corporate social responsibility requirements as the Authority may notify to the Supplier from time to time.

**2. Equality and Accessibility**

- 2.1 Without prejudice to the generality of its rights and obligations under each Contract, the Supplier shall support the Authority in fulfilling its public sector equality duty under S149 of the Equality Act 2010 by ensuring, so far as reasonably practicable, that it (the Supplier) fulfils its obligations under each Contract in way that has due regard to the need to:
  - 2.1.1 Eliminate discrimination, harassment or victimisation and any other conducted that is prohibited under the 2010 Act; and
  - 2.1.2 Advance equality of opportunity and foster good relations between those who share a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

**3. Modern Slavery, Child Labour and Inhumane Treatment**

The "Modern Slavery Helpline" refers to the point of contact for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at <https://www.modernslaveryhelpline.org/report> or by telephone on 08000 121 700.

**3.1 The Supplier:**

- 3.1.1 Shall not use, or allow its Subcontractors to use, forced, bonded or involuntary prison labour;
- 3.1.2 Shall not require any Supplier staff or Subcontractor staff to lodge deposits or identify papers with the Employer or deny Supplier staff freedom to leave their employer after reasonable notice;
- 3.1.3 Warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.
- 3.1.4 Warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offenses anywhere around the world.
- 3.1.5 Shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offences anywhere around the World.
- 3.1.6 Shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act 2015 and shall include in its contracts with its subcontractors anti-slavery and human trafficking provisions;
- 3.1.7 Shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;
- 3.1.8 Shall prepare and deliver to the FCDO at the commencement of each Contract and updated on a frequency defined by the Authority, a slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business;
- 3.1.9 Shall not use, or allow its employees or Subcontractors to use, physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;
- 3.1.10 shall not use, or allow its Subcontractors to use, child or slave labour;
- 3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to the Authority and Modern Slavery Helpline.

**4. Income Security****4.1 The Supplier shall:**

- 4.1.1 Ensure that that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;
- 4.1.2 Ensure that all workers are provided with written and understandable information about their terms and conditions of employment, and in particular in respect of wages, before they enter employment, and about the particulars of their wages for the pay period concerned each time that they are paid;

- 4.1.3 Not make deductions from wages as a disciplinary measure except
  - (a) Where permitted by law; and
  - (b) Upon express permission of the worker concerned.
- 4.1.4 Record all disciplinary measures taken against Supplier Staff throughout the term of each contract; and
- 4.1.5 Ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

## 5. Working Hours

5.1 The Supplier shall:

- 5.1.1 Ensure that the working hours of Supplier staff comply with national laws, and any collective agreements;
- 5.1.2 Ensure that the working hours of Supplier staff, excluding overtime, are defined by contract, and do not exceed 48 hours per week unless the individual has lawfully agreed so in writing;
- 5.1.3 Ensure that overtime is used responsibly, taking into account:
  - (a) The extent;
  - (b) Frequency; and
  - (c) Hours worked
 By reference to individuals and the Supplier staff as a whole;

5.2 The total hours worked by an individual in any seven-day period shall not exceed 60 hours, unless the criteria set out in paragraph 5.3 are satisfied.

5.3 Working hours may exceed 60 hours in any seven-day period only where all of the following are met:

- 5.3.1 This is allowed by national law;
- 5.3.2 This is expressly authorised by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;
- 5.3.3 Appropriate safeguards are taken to protect the workers' health and safety; and
- 5.3.4 The employer can demonstrate that exceptional circumstances apply.

5.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.

## 6. Sustainability

6.1 The Supplier shall meet the applicable [Government Buying Standards](#) applicable to Deliverables.

**SUPPLIER BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN**  
[REDACTED]

**Appendix I**

## Section 3 - Statement of Service Requirements

### 1. PURPOSE

1.1 The current Hardship and Cost of Living Data Processing & Provision contract will end on 14 April 2024. We (the Foreign, Commonwealth & Development Office, hereafter referred to as 'the Authority') are offering one contract, awarded through an open competition, for future provision of this service.

### 2. BACKGROUND TO THE CONTRACTING AUTHORITY

2.1 The Foreign, Commonwealth and Development Office, more commonly known as the FCDO is a ministerial department supported by 11 agencies, including FCDO Services and the British Council. The FCDO works to pursue our national interests and project the UK as a force for good in the world. We promote the interests of British citizens, safeguard the UK's security, defend our values, reduce poverty and tackle global challenges with our international partners.

2.2 We unite development and diplomacy in one department. FCDO brings together the best of Britain's international effort and demonstrates the UK acting as a force for good in the world.

2.3 We employ around 17,300 staff in our diplomatic and development offices worldwide, including in 280 overseas Embassies and High Commissions. Our UK-based staff work in King Charles Street, London and Abercrombie House, East Kilbride. We also have other London offices, including 22 Whitehall, and staff based in Milton Keynes.

### 3. BACKGROUND TO THE REQUIREMENT/OVERVIEW OF THE REQUIREMENT

3.1 The Authority has a requirement for the collation, checking and distribution of worldwide Hardship and Cost of Living information for our Posts and overseas Missions. The Hardship element is more commonly referred to as a Location Allowance. The data gathered in this exercise will be used to calculate the Hardship element of Diplomatic Service Allowance (DSA) and Cost of Living Allowance (COLA) that the FCDO provides to its staff serving overseas.

#### 3.2 Other Government Departments:

3.3 This will be a One HMG contract with service provision available to all Central Government Departments, their Executive Agencies and their Non Departmental Public Bodies (NDPBs), and any successors. Historically, only Partners Across

Government (PAGs) on the overseas platform have required this or a similar service – cf. **ANNEX 2 – PARTNERS ACROSS GOVERNMENT ON THE ONE HMG OVERSEAS PLATFORM.**

3.4 The FCDO will be the Contract Authority and the Statement of Service Requirements, Technical Evaluation Questions, and Pricing Model reflect FCDO requirements. PAGs may require some adaptation by direct arrangement with the Potential Provider.

3.5 PAGs will be required to sign a Memorandum of Understanding with the FCDO, which will cover prompt payment and performance management requirements and expectations.

3.6 It should also be noted that work is underway to align, as far as possible, international allowances for staff working for HMG internationally, following the Prime Minister setting out in 2020 the intention that "all staff in country, whether posted or locally engaged, should be on the same terms and conditions and treated equally". In the event that this work concludes during the contract term, it is possible that PAG requirements may be varied into this contract as their direct arrangements, either with the Existing or Potential Provider, expire.

#### 3.7 Mobilisation and transition arrangements:

3.8 The Authority estimates that the contract mobilisation period between contract award and contract start date will be c. 3 months.

3.9 IHR, in partnership with Authority Commercial colleagues, will work with the Potential Provider on contract award to agree a mobilisation plan for implementation.

3.10 In the event of a service transition, the Potential Provider will be expected to work with the Existing Provider throughout this period and must be fully available for detailed transition and planning from the date of the Authority's notification of Intention to Award a contract.



3.11 The same collaborative transition approach is expected to apply should any similar transition be required at the end of this contract to any Future Provider.

#### 4. DEFINITIONS

Expression or Acronym	Definition
CBS	Country Based Staff are those employed locally by the British Embassy or High Commission (or other Diplomatic Office in country).
UKBS	UK Based staff are those employed by the FCDO in the UK and have a UK based contract.
COLA	Cost of Living Location Allowance
FCDO	Foreign, Commonwealth & Development Office
HMT	His Majesty's Treasury
IHR	International HR, Human Resources Directorate, FCDO
PAG	Partner Across Government/Other Government Department
Post	British Embassy, High Commission or Consulate
Hardship Post	A Post where living conditions are difficult due to security, climate, healthcare and other factors. The FCDO pays staff a Hardship allowance to compensate them for maintaining quality of life in these challenging environments.
Subordinate Post	In addition to the main diplomatic office (Embassy or High Commission), some countries also have one or more 'subordinate Posts' these are often Consulates or Deputy High Commissions.

#### 5. THE REQUIREMENT

##### Hardship Allowance:

5.1 A Hardship Allowance is paid to compensate staff and their families for the additional costs of maintaining quality of life at hardship Posts. It also provides compensation for the wider challenges that officers face in locations globally when compared to life in the UK and working in London.

5.2 The authority requires the Potential Provider to conduct an annual survey (or other method of assessment) for all FCDO Posts (cf. **ANNEX 1 – FULL LIST OF FCDO POSTS**), to assess the challenges affecting staff relocating to those countries. A ranking/scoring system should be provided by the Potential Provider setting out clearly the reasoning's behind the system and any scores to enable calculation of the final allowances payable based on their methodology. It needs to be modern and inclusive in design, to take account of an ever-changing internationally mobile workforce. Currently the Hardship Allowance is reviewed annually (on 1 February), therefore the Potential Provider would be expected to provide the Authority with Hardship Scores by November each year to allow time for any new rates to be implemented. A Hardship and COLA assessment is required for all FCDO Posts. However, many will not meet the qualifying threshold to receive these allowances.

5.3 Data-gathering/methodology: Any location details collected from FCDO staff ( i.e. via a survey) should include, Country/territory of assignment, name of town/city/state, and family status on assignment (leave

blank if you prefer not to say): Accompanied by partner and children, Accompanied by partner only, accompanied by children only and Not Applicable if a non-accompanied location. Annex 3 provides current/historic methodology for calculating Hardship Allowances, including categories currently assessed, which suppliers may wish to consider.

5.4 The methodology and calculations need to be robust as they are often subject to challenge by assignees in country, who live and work there. The Potential Provider is required to create a survey or other method that will enable them and the authority to defend any challenge to the methodology implemented and to evidence how they assessed the challenges faced by expatriate populations in the country generally or specific locations where the authority has staff working and set out how different conditions may be impacting the lifestyle of those who agree to work in different parts of the globe.

5.5 Data should be collected from multiple primary and secondary sources to ensure its accuracy and reliability and the supplier should ensure that any calculations undertaken on behalf of the Authority adhere to FCDO policy. The supplier should be able to provide detailed explanations of why, when and how a hardship rating has changed, putting the complexities of the challenges at each location into a simple explanation as to why an employee's allowance has changed.

5.6 We would expect the potential provider to draw on a range of sources and expertise to collect and collate the data, to ensure the lived in and local context in any given country is reflected in the analysis, data and recommendations. For example this could include accessing information from assignees (FCDO staff and others) who live and work in each location, regular spot checks on locations or the use of open source information. It is important that the information is robust and reflects the 'lived experience' of that particular country. This ensures the data provided remains relevant as the location's environment changes.

#### Cost of Living Allowance (COLA):

5.7 FCDO pays its UK-based staff serving overseas a Cost of Living Allowance (COLA) to compensate them for the additional costs of maintaining a standard of living comparable to the UK. The cost of living uplift is not sufficient on its own to cover local living costs and is not intended to be an incentive to work at any particular Post. COLA is paid with salary as a tax-free non-consolidated allowance. HMT closely scrutinise these allowances; providing challenge to help ensure the payments do not act as an incentive to work overseas.

5.8 Rates of COLA vary from one country to another and are paid dependent on family circumstances. In some countries where the cost of living is cheaper than in the UK, it may be the case that COLA is zero rated.

5.9 Data-gathering/methodology: The Potential Provider will be required to design and implement an appropriate, tested and accurate method to calculate the Cost of Living Allowance or Uplift, for any UK overseas mission with FCDO UK-Based Staff and in any additional locations where UK Based FCDO staff may be located in the future.

5.10 All country data sets should include country specific details, such as the location, currency used for purchasing, exchange rates at time of completing survey, date of survey completion, and if/where sales (e.g. value added) tax is included.

5.11 It may be necessary to design a survey and shopping basket of items that are commonly available and purchased in the UK. This should include items such as common groceries, cooking utensils, toiletries, mobile phones, computers or other items that the Potential Provider defines as necessary to maintain a lifestyle comparable to the UK and would be on a normal shopping list for day-to-day purchases in the UK. Other methods can be proposed to calculate the COLA. Potential Providers may base this on open source information, such as Gov.UK data, or other sources to create an index for the COLA rates being set. Where Potential Providers wish to use other methods to calculate the COLA, they need to fully demonstrate these options and how they will work. Bearing in mind use of open source data may not be available for some locations where access to data is restricted. Approaches, methodologies, and quality assurance for data collection and data analysis will be assessed as part of the Technical Evaluation. The proposed solution will need to be built and tested and ready to deploy by contract start date (15 April 2024). The Authority estimates that the contract mobilisation period between contract award and contract start date will be c. 3 months.

5.12 **Calculation:** For consistency the Potential Provider will where possible need to set the rates against a set date, prior to the provision of the new data, setting out what exchange rates are used on that date for each location. The Potential Provider will need to take into consideration that the FCDO also pays what are referred to as assignment costs, these relate to the use of recreational facilities like clubs, gyms, child care or babysitting, domestic help and international telephone calls. Not all assignments costs are paid to all

employees e.g. those residing in accommodation that is used for official functions have certain payments deducted.

5.13 Data should have a base rate for expenditure, set against the Cost of Living in the UK (Outer London), the cost of goods need to be compared to the same or similar items in the UK, to establish an index of prices - where the 100% mark is set against the UK costs, so that staff are not over compensated for the additional costs that might be incurred and considered an incentive to work in some countries.

5.14 All data should be examined and may be subject to challenge, the Potential Provider may therefore need to be able to undertake some cross checking of pricing, where data is supplied through a survey. If no survey is conducted then the research behind the data will need to robustly set out how figures have been calculated and demonstrate the validity of the research methods.

**5.15 COLA output data - Explanations of the changes in COLA Rates:** The Potential

Provider will be required to provide detailed explanations of the rises or decreases in COLA in a suitably brief format which sets out what has influenced the change; be that exchange rate, inflation or other factors. This could be a PDF document covering general changes. More detailed changes may be required to be set out for Posts seeing increases or decreases at review points.

5.16 **Interim Reviews.** The Potential Provider will need to offer an 'early warning system' providing details and summary explanations of any locations likely to face a review, explaining if any change is inflation or exchange rate based, and notifying the authority in advance which Posts will see an increase and which Posts will see a decrease. The information provided will enable the authority to decide if there is to be an interim review and further decide if the changes are to be implemented. In such cases, the Potential Provider will provide new rates for all affected locations, plus detailed explanations which set out the reasoning behind any increase or decrease. Scenarios in which interim COLA data may be required include but are not limited to:

5.16.1 Changes in exchange rates for sterling to local currency over a period of 8 weeks, could be due to various factors, such as devaluation of currency or strengthening of one currency against the other of more than 10% plus or minus;

5.16.2 Post now having UK Based Staff based in new locations, so requiring COLA and Hardship Assessments;

5.16.3 Changes in the country currency, that could be adopting the Euro or changes to a new currency/denominations causing exchange rate fluctuations.

5.17 **COLA output data - Data Sets:** To be supplied for each change or review – data that fully sets out the COLA and Assignment Costs, based on pay bands as set/agreed with the Potential Provider. One data set is to be based around a spreadsheet detailing the factors for all locations, published in alphabetical order. A separate data set should include a spreadsheet for each individual location. All data should include the indexes used, exchange rates used and the date of exchange rate set for the calculations, showing pay bands for each, if accompanied or single officer rate, child element of the COLA and the child elsewhere rates applied. The Potential Provider will provide updated versions of both these data sets to the authority for each review or interim review.

5.18 Cf. **ANNEX 3 – CURRENT/HISTORIC METHODOLOGIES FOR CALCULATING COST OF LIVING ALLOWANCES AND HARDSHIP ALLOWANCES** for an overview of how these services are currently being/have historically been delivered.

## 6. KEY MILESTONES

6.1 The Potential Provider should note the following project milestones that the Authority will measure the quality of delivery against:

Milestone	Description	Timeframe
Contract mobilisation/transition	<ul style="list-style-type: none"> <li>Potential Provider to produce contract mobilisation/transition plan - including: activities, timings and RASCI (responsible, accountable, supportive, consulted, informed) assignments – to include Authority and/or the Existing Provider (in the event of a service transition) as required – and agree with Authority.</li> <li>Potential Provider to produce change communications plan and agree with Authority.</li> <li>Authority/Potential Provider contract mobilisation reporting and meetings (to be agreed on contract award)</li> <li>Proposed solution built and tested (sample Hardship location scores and Cost of Living Allowance rates to be provided for a number of</li> </ul>	<p>Contract award-contract start date (15 April 2024):</p> <ul style="list-style-type: none"> <li>Contract mobilisation/transition plan to be agreed within 2 weeks of contract award.</li> <li>Change communications plan to be agreed within 1 month of contract award.</li> <li>Contract mobilisation reporting and meetings to be agreed within 2 weeks of contract award.</li> <li>Proposed solution built and tested and ready to deploy by contract start date (15 April 2024).</li> <li>All staff who will work on the contract in place and trained by</li> </ul>
	<p>Posts – to be agreed on contract award).</p> <ul style="list-style-type: none"> <li>Staffing: All Potential Provider staff who will work on the contract to be in place and trained.</li> <li>Data Protection/Cyber Security/Personnel Security actions as required – cf. 13. SECURITY REQUIREMENTS.</li> </ul>	contract start date (15 April 2024).
Provision of interim Cost of Living Allowance (COLA) rates - June	Cf. 4. THE REQUIREMENT.	To be delivered as required from contract start date (15 April 2024).

Management and Key Performance Indicator Review Meetings	Cf. 12. REPORTING.	End-June 2024 then quarterly thereafter (endSeptember, endDecember, end-March etc.)
Provision of Cost of Living Allowance (COLA) rates - September	Cf. 4. THE REQUIREMENT.	To be finalised and submitted to the Authority by September 2024.
Provision of Hardship location scores	Cf. 4. THE REQUIREMENT.	To be finalised and submitted to the Authority by November 2024.
Provision of interim Cost of Living Allowance (COLA) rates - December	Cf. 4. THE REQUIREMENT.	To be delivered as required.
Provision of Cost of Living Allowance (COLA) rates - March	Cf. 4. THE REQUIREMENT.	To be finalised and submitted to the Authority by March 2025.

## 7. AUTHORITY'S RESPONSIBILITIES

7.1 The Authority will provide the Potential Provider with the names of all locations where FCDO UK Based staff are posted along with details of any revisions following naming convention changes as well as details of any additional locations, should new Posts open.

7.2 The Authority will establish key points of contact within the FCDO for liaison purposes and respond to enquiries by the Potential Provider within a reasonable period, setting out responses or potential delays in providing a full response.

7.3 The Authority will promote the survey and survey dates (if applicable) as and when informed by the Potential Provider. The Authority will communicate within the FCDO when any surveys are open or due to open, to enable participation by staff within the FCDO.

7.4 The Authority will inform the Potential Provider of any changes to the service or data required, to enable Potential Provider to revise the formats of surveys/data output or add details to location lists (i.e. any changes following FCDO policy changes or alignment work). The Authority will work with the Potential Provider to agree a suitable time period to allow for any changes to be implemented.

## 8. KEY PERFORMANCE INDICATORS AND SERVICE CREDITS

8.1 The Authority will measure the quality of the Potential Provider's delivery using the below Key Performance Indicators, which the Potential Provider will be expected to achieve and against which the Potential Provider's performance will be assessed. These will be reviewed as part of quarterly Management and Key Performance Indicator Review Meetings between the Authority and the Potential Provider. This will allow any disputes and/or questions around methodology or evaluation to be raised and discussed. The Authority will have the final decision.

8.2 It must be noted that all requirements included in the STATEMENT OF SERVICE REQUIREMENTS are key to successful service delivery. The Authority therefore reserves the right to upgrade any requirements included to a Key Performance Indicator, or to introduce a Service Credit, at any point during the term of the contract if we feel that any part of the service is not being delivered to the required standard, and do not expect any reasonable additions to be rejected.

Key Performance Indicator	Service Area	Description	Target	Service Credit
1	Delivery – Hardship data to be provided annually	Hardship data to be provided by November each year in advance of Authority publication of hardship scores in February.	100%	<p>Pass/fail to be confirmed annually.</p> <p>Potential Provider to specify in <b>PRICING MODEL</b> % (between 10 and 20) of Total Fixed Price (£) for Hardship data/all data sets to be put at risk/deducted in the event that &lt; 100% of all Hardship data sets are provided on time - to be used for the annual payment.</p> <p>Exact deadline, Authority responsibilities, and</p>
				clock starts and stops to be agreed with the Potential Provider on contract award.

2	Delivery – COLA data to be provided twice yearly	COLA data to be provided twice yearly in September and March each year in advance of Authority COLA review delivery dates.	100%	<p>Pass/fail to be confirmed in September and March each year respectively.</p> <p>Potential Provider to specify in <b>PRICING MODEL</b> % (between 10 and 20) of Total Fixed Price (£) for Cost of Living Allowance data/all data sets to be put at risk/deducted in the event that &lt; 100% of all Cost of Living Allowance (COLA) data sets are provided on time - to be used for the March worldwide costing exercise and September update payments respectively.</p> <p>Exact deadline, Authority responsibilities, and clock starts and stops to be agreed with the Potential Provider on contract award.</p>
3	Delivery – interim COLA data, including ad hoc/out-ofcycle data sets, to be provided within 8 weeks of request	Interim COLA data to be provided within 8 weeks of request by the Authority.	100%	<p>Pass/fail to be confirmed in June and December each year respectively.</p> <p>Potential Provider to specify in <b>PRICING MODEL</b> % (between 10 and 20) of Total Fixed Price (£) for Cost of Living Allowance data/all data sets to be put at risk/deducted in the event that &lt; 100% of all Cost of Living Allowance (COLA)</p>

				<p>data sets are provided on time - to be used for the June interim review and any ad hoc/out-of-cycle data sets delivered January/June, and December interim review and any ad hoc/out-of-cycle data sets delivered July-December payments respectively.</p> <p>Exact deadline, Authority responsibilities, and clock starts and stops to be agreed with the Potential Provider on contract award.</p>
4	Reporting – Potential Provider to provide a clear and easy-to-understand analysis and recommendation report to explain change in Hardship/COLA figure	<p>A detailed explanation of why, when, and how a Hardship/COLA figure has changed to be provided. The explanation provided should be presented in an easy-to-understand format to be agreed with the Potential Provider on contract award. The report should draw on the wider global economic and security context and proximity analysis.</p>	100% of the time (ad hoc requirement)	N/A
5	Customer service – Potential Provider to address	Authority queries and questions about any aspect of the overall	100% of the time (ad hoc requirement)	N/A



	Authority queries and questions within 3 working days	service resolved within 3 working days. If queries will require longer than 3 working days to resolve, the Potential Provider should set out the action(s) being taken to resolve, including timings, and keep the officer and/or IHR aware (as appropriate).		
6	Social Value – Key Performance Indicator to be agreed with Potential Provider on contract award	TBA	TBA	N/A

## 9. STAFFING

9.1 The Potential Provider will be required to provide a sufficient level of resource throughout the duration of this contract to ensure effective and consistent delivery, including: accuracy of data and quality of analysis, timeliness of delivery, quality of explanations and reporting, responsiveness, and innovation and continuous improvement. Resource with relevant qualifications, experience and expertise may include:

- 9.1.1 Qualified economic data analysts;
- 9.1.2 Global economic and security expertise;
- 9.1.3 IT and data security management.

9.2 The Potential Provider will ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

9.3 The Potential Provider will be required to provide a **designated Senior Single Point of Contact** for resolution of contract variations, legal and financial issues, and serious complaints, also responsible for:

- 9.3.1 Employment contracts, and discipline and performance of all staff directly working on the contract; and any third-party sub-contractors employed by the Potential Provider on behalf of the Authority;
- 9.3.2 Overall level of service provision to Authority;
- 9.3.3 Overall Delivery Risk Management;
- 9.3.4 Discipline and performance of all staff directly working on the contract; and any third-party sub-contractors employed by the Potential Provider on behalf of the Authority.

9.4 A suitably-empowered alternative contact should be nominated when the Senior Single Point of Contact will be out of office for more than 3 days.

9.5 The Main Provider will be required to provide a **designated working-level Single Point of Contact** for oversight of the delivery of the below responsibilities:

- 9.5.1 Continuous improvement of data accuracy and efficiency, including ways in which the data and systems can be more efficiently administered and delivered;
- 9.5.2 Communications and engagement with FCDO or PAG staff, dependants and or FCDO missions and platforms;
- 9.5.3 Performance management of any systems or data links with FCDO or PAG IT systems and teams;
- 9.5.4 High Risk Global, regional and country level economic outlook and analysis proximity warning briefing Economic analysis and data interpretation for quality control and as needed by the Authority;
- 9.5.5 Communications and engagement with FCDO or PAG staff, dependants and or FCDO missions and platforms;
- 9.5.6 Performance management of any systems or data links with FCDO or PAG IT systems and teams;
- 9.5.7 Delivery Risk Management.

9.6 A suitably-empowered alternative contact should be nominated when the Single Point of Contact will be out of office for more than 3 days.

9.7 The Potential Provider will be required to provide a **designated Single Point of Contact for financial queries**, including queries regarding invoices. A suitably-empowered alternative contact should be nominated when the Single Point of Contact will be out of office for more than 3 days.

## 10. CUSTOMER SERVICE

10.1 The Potential Provider will be required to address Authority queries and questions within 3 working days about any aspect of the overall service.

10.2 If queries will require longer than 3 working days to resolve, the Potential Provider should set out the action(s) being taken to resolve, including timings, and keep the officer and/or IHR aware (as appropriate).

10.3 The Potential Provider will be required to flag issues to the Authority as early as possible and keep the Authority informed of workarounds and process deviations where required.

## 11. INNOVATION AND CONTINUOUS IMPROVEMENT

11.1 The Potential Provider will be expected to continually improve the way in which the required Services are to be delivered throughout the contract duration.

11.2 The Potential Provider should set out their approach to working with the Authority to monitor performance and approach and evaluate and implement changes. The Potential Provider should consider the approach to ensuring the end product benefits from innovation and advances in technology and understanding of the Authority's vision and long term goals during Management and Key Performance Indicator Review Meetings.

11.3 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

11.4 Example areas where potential Providers could demonstrate their thinking on innovative approaches include:

11.4.1 Ways to reduce the administration burden on the Authority in administering the allowance packages including ways to reduce critical pinch point pressures and smarter automation.

11.4.2 Providing innovative early warning digital dashboards and real time data analysis to reduce the risk of data delay, and/or multiple meetings and reporting formats;

- 11.4.3 Innovative ways to support the Authority make the allowance and hardship scores more accurate and reflective of reality in complex and unpredictable contexts.
- 11.4.4 Innovations associated with capturing more complete and accurate data and information on the ground, reducing time and effort and providing a secure way of gathering mass data (where applicable, safe and/or where possible)
- 11.4.5 Smarter IT and data transfers methodology to reduce pinch points, improve compatibility, improve data accuracy and speed up dataset compilation
- 11.4.6 Ability to flex and adapt the contract to provide VFM for other PAGs who may want to join the contract.
- 11.5 The FCDO continually reviews its internal processes and policies to ensure they accurately reflect the needs of a modern global workforce. As our allowances continue to evolve, it is possible that 'assignment costs' or the 'shopping basket' could change in the future. Any changes to policy that would affect the calculation of COLA by the Potential Provider will be communicated sufficiently in advance of any COLA exercise being undertaken.

## 12. SOCIAL VALUE AND SUSTAINABILITY

12.1 The Authority has identified 'effective stewardship of the environment' as the Social Value Policy Outcome for this procurement. Cf. Cabinet Office guidance, information and resources regarding the Public Services (Social Value) Act

2012:<https://www.gov.uk/government/publications/social-value-act><https://www.gov.uk/government/publications/social-value-act-information-and-resources/social-value-act-information-and-resources>information-and-resources/social-value-act-information-and-resources

12.2 This Act requires English and Welsh public authorities (subject to some exclusions in relation to Welsh authorities) to consider, at the pre-procurement (preparation and planning) stage:

12.2.1 How what is proposed to be procured might improve the economic, social and environmental wellbeing of the relevant area;

12.2.2 How, in conducting the process of procurement, it might act with a view to securing that improvement; and

12.2.3 Whether to undertake any consultation on the above.

12.3 Bidders will be required to respond to a Technical Evaluation Question to describe the commitment your organisation will make to ensure that opportunities under the contract deliver the Social Value Policy Outcome 'improve health and wellbeing' and Model Award Criteria of:

12.3.1 MAC 4.1 Deliver additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas emissions.

12.3.2 MAC 4.2 Influence staff, Potential Providers, customers and communities through the delivery of the contract to support environmental protection and improvement.

12.4 The Potential Provider will be expected to demonstrate sustainability and social value based on industry best practice and in line with UK Government sustainability, greening and UK Net Zero goals. This includes commitments to: minimise energy demands in the collection, storing and transmission of data; and alignment with the UK Government's Data Ethics Framework. The Potential Provider should also outline their approach to monitoring and improving their sustainability performance and approach over the lifetime of the contract to bring online innovative ways to increase efficiency, save resources and maintain effectiveness for both Potential Provider and the Authority. This might include identifying ways the Authority can use the data and analysis to meet the FCDO's own sustainability targets and/or ways to either collect and analyse data or minimise staff administration time.

12.5 The Potential Provider should consider the approach to data collection to ensure a fair, equitable and inclusive data and analysis reflecting the diversity, welfare and work-life balance of our Staff, families and dependants serving the UK overseas.

## 13. REPORTING

13.1 The Potential Provider will report to IHR.

13.2 The Potential Provider will be required to attend quarterly Management and Key Performance Indicator Review Meetings, and any other meetings as requested by the Authority. The Potential Provider will also be required to agree and record actions arising and take forward actions arising.

13.3 The Potential Provider is required to provide an accurate and comprehensive Management and Key Performance Indicator Review Report to the Authority at least 5 working days in advance of the respective meetings throughout the life of the contract.

13.4 Contents of the Management and Key Performance Indicator Review Report should include:

13.4.1 Data and analysis quality assurance updates; management meeting to quality check data provided via a spot check of 10 Post/locations

13.4.2 Delivery risk management, including: potential and/or actual delivery risks, action(s) being taken to mitigate or manage, and contingency planning/workaround to be used as appropriate;

13.4.3 Anticipation of Hardship location score and/or Cost of Living Allowance (COLA) rate revision requirements, including: economic and context forecasting and analysis, providing a deeper dive on any locations identified as being of interest by the Authority or Potential Provider;

13.4.4 Innovation and continuous improvement suggestions/Monitoring, Evaluation, Research, and Learning updates;

13.4.5 Staffing updates as appropriate;

13.4.6 Social Value updates;

13.4.7 Performance against KPIs and commentary.

13.5 To note, a full reporting list and format of delivery will be agreed with the Potential Provider upon appointment.

## 14. SECURITY REQUIREMENTS

14.2 **Data Protection:** All data held on behalf of the Authority in relation to this contract must be held within the United Kingdom. The Potential Provider will need to set out how they will manage Authority data to prevent non-authorized staff from accessing this. A Business Continuity and Disaster Recovery Plan will be required to safeguard the authority's data in the event of IT systems failure, including system corruption, or loss of data e.g. due to hacking. The

Potential Provider may be required to work with the Authority on contract award to complete a Data Protection Impact Assessment, as appropriate to the solution proposed.

14.3 **Cyber Security:** We invite bidders to propose technological initiatives in any area of our requirement that could improve the service to FCDO while making potential savings. The Potential Provider may be required to work with the Authority on contract award to agree minimum cyber security requirements, as appropriate to the solution proposed. Cf. **APPENDIX 1 – AUTHORITY CYBER SECURITY REQUIREMENTS** for indicative requirements.

14.4 **Personnel Security:** We do not anticipate Potential Provider staff working on this contract to require security clearance, however, we will be required to review the solution proposed and confirm this on contract award.

14.5 **Confidentiality:** The successful bidder and any employees or sub-contractors will be required to sign a Confidentiality Undertaking. Cf. Appendix B of **CONTRACT TERMS AND CONDITIONS** attachment.

## 15. PRICES AND VOLUMES

15.1 The contract will have a number of chargeable elements. Cf. **PRICING MODEL** attachment for completion by the Potential Provider.

16.2 Specifically, we will seek to clarify the following fixed prices:

16.2.1 Provision of Hardship data set/per location rate (annual requirement);

16.2.2 Provision of Cost of Living Allowance (COLA) data set/per location rate (to be used for March worldwide costing exercise, June interim review, September update, December interim review, and any ad hoc/out-of-cycle data sets).

16.3 The fixed prices to be stated in tab 2. Schedule of Prices and Rates constitute the only amounts payable by the Authority to the Potential Provider for providing the services. The fixed prices shall include all costs and expenses incurred either directly or indirectly by the Potential Provider in providing the services, including (but not limited to) staffing, mobilisation, transition, and provision of Management and Key Performance Indicator Review reporting and attendance at meetings and presentations as required by the Authority. Therefore, these rates should be sustainable for Potential Providers throughout the life of the contract.

16.4 Value for Money: The Potential Provider undertakes to make all reasonable efforts to ensure that all services are delivered at the best possible market price, in line with the Authority's requirements to ensure Value for Money. For the purpose of this contract, Value for Money is defined as the optimum combination of whole life costs and quality to meet the Authority's requirements.

16.5 Price Adjustment: Total cost for Years 6 and 7 will be subject to C4. PRICE ADJUSTMENT in the CONTRACT TERMS AND CONDITIONS attachment

(fixed prices will remain unchanged for a period of five years, thereafter indexation may be applied, as agreed by both parties).

16.6 Commercial evaluation: The Authority's commercial evaluation will be based on 'Total cost over seven years - based on pricing scenario', to enable like-for-like pricing consideration.

16.7 Volumes: For the deliverables 'Provision of Hardship data (annual requirement)', 'Provision of Cost of Living Allowance (COLA) data - March worldwide costing exercise', and 'Provision of Cost of Living Allowance (COLA) data - September update', the Authority has used the cost assumption that 282 data sets will be required in each case. For the deliverables 'Provision of Cost of Living Allowance (COLA) data - June interim review' and 'Provision of Cost of Living Allowance (COLA) data - December interim review', the Authority has estimated that 25 data sets will be required in each case, based on the previous year. However, the Authority does not guarantee this volume of activity as requirements can vary year-on-year.

## 16. PAYMENT

17.1 The PRICING MODEL attachment includes a Payment Plan for completion by the Potential Provider.

17.2 Payment will be by BACS on receipt of a valid invoice.

## 17. ANNEXES

**18.1 ANNEX 1 – FULL LIST OF FCDO POSTS**

**18.2 ANNEX 2 – PARTNERS ACROSS GOVERNMENT ON THE ONE HMG OVERSEAS PLATFORM**

**18.3 ANNEX 3 – CURRENT/HISTORIC METHODOLOGIES FOR CALCULATING COST OF LIVING ALLOWANCES AND HARDSHIP ALLOWANCES**

## 18. ANNEX 1 – FULL LIST OF FCDO POSTS

A full list of FCDO Posts is published on [Gov.uk](https://www.gov.uk). The list is subject to change as new Posts open or Posts close and is therefore updated regularly.

A Hardship and COLA assessment is required for all FCDO Posts. However, many will not meet the qualifying threshold to receive these allowances.

<u>Region</u>	<u>Country</u>	<u>Post</u>
Africa	Ivory Coast	Abidjan
MENA & AfPak	United Arab Emirates	Abu Dhabi
Africa	Nigeria	Abuja
Africa	Ghana	Accra
Americas and Overseas Territories	Pitcairn Islands	Adamstown
Africa	Ethiopia	Addis Ababa
Indo-Pacific	India	Ahmedabad
MENA & AfPak	Algeria	Algiers
Europe	Spain	Alicante
Eastern Europe & Central Asia	Kazakhstan	Almaty
MENA & AfPak	Jordan	Amman
Europe	Turkey	Ankara
Europe	Turkey	Antalya
Africa	Madagascar	Antananarivo
Indo-Pacific	Samoa	Apia
Americas and Overseas Territories	Ascension	Ascension Island
Eastern Europe & Central Asia	Turkmenistan	Ashgabat
Africa	Eritrea	Asmara
Eastern Europe & Central Asia	Kazakhstan	Astana
Americas and Overseas Territories	Paraguay	Asuncion
Europe	Greece	Athens
Americas and Overseas Territories	United States of America	Atlanta
Indo-Pacific	New Zealand	Auckland
MENA & AfPak	Iraq	Baghdad
Eastern Europe & Central Asia	Azerbaijan	Baku
Indo-Pacific	Indonesia	Bali
Africa	Mali	Bamako

Indo-Pacific	Brunei	Bandar Seri Begawan
Indo-Pacific	Thailand	Bangkok
Europe	Bosnia	Banja Luka
Africa	Gambia (The)	Banjul
Europe	Spain	Barcelona
Indo-Pacific	China	Beijing
MENA & AfPak	Lebanon	Beirut
Europe	Serbia	Belgrade
Americas and Overseas Territories	Belize	Belmopan
Americas and Overseas Territories	Brazil	Belo Horizonte
Indo-Pacific	India	Bengaluru
Europe	Germany	Berlin
Europe	Switzerland	Berne
Europe	Spain	Bilbao
Eastern Europe & Central Asia	Kyrgyzstan	Bishkek
Americas and Overseas Territories	Colombia	Bogota
Europe	France	Bordeaux
Americas and Overseas Territories	United States of America	Boston
Americas and Overseas Territories	Brazil	Brasilia
Europe	Slovakia	Bratislava
Americas and Overseas Territories	Barbados	Bridgetown
Indo-Pacific	Australia	Brisbane
Europe	Belgium	Brussels Embassy
Multilateral	Belgium	Brussels UKDEL NATO
Multilateral	Belgium	Brussels UKMIS
Europe	Romania	Bucharest
Europe	Hungary	Budapest
Americas and Overseas Territories	Argentina	Buenos Aires
Africa	Burundi	Bujumbura

MENA & AfPak	Egypt	Cairo
Americas and Overseas Territories	Canada	Calgary
Indo-Pacific	Australia	Canberra
Americas and Overseas Territories	Mexico	Cancun
Africa	South Africa	Cape Town
Americas and Overseas Territories	Venezuela	Caracas
MENA & AfPak	Morocco	Casablanca
Americas and Overseas Territories	St Lucia	Castries
Indo-Pacific	India	Chandigarh
Indo-Pacific	India	Chennai
Americas and Overseas Territories	United States of America	Chicago
Eastern Europe & Central Asia	Moldova	Chisinau
Indo-Pacific	China	Chongqing
Indo-Pacific	Sri Lanka	Colombo
Africa	Guinea	Conakry
Europe	Denmark	Copenhagen
Europe	Greece	Corfu
Africa	Senegal	Dakar
MENA & AfPak	Syria	Damascus (Syria Overseas Network)
Africa	Tanzania	Dar es Salaam
Americas and Overseas Territories	United States of America	Denver
Indo-Pacific	Bangladesh	Dhaka
Africa	Djibouti	Djibouti
MENA & AfPak	Qatar	Doha
MENA & AfPak	United Arab Emirates	Dubai
Europe	Ireland	Dublin
Eastern Europe & Central Asia	Tajikistan	Dushanbe
Europe	Germany	Dusseldorf
Africa	Nigeria	Enugu



MENA & AfPak	Iraq	Erbil
Europe	Turkey	Fethyie
Africa	Sierra Leone	Freetown
Africa	Botswana	Gaborone

MENA & AfPak	Occupied Palestinian Territories	Gaza
Multilateral	Switzerland	Geneva UKDIS
Multilateral	Switzerland	Geneva UKMIS
Americas and Overseas Territories	Guyana	Georgetown
Europe	Gibraltar	Gibraltar
Indo-Pacific	India	Goa
Africa	Democratic Republic of the Congo	Goma
Americas and Overseas Territories	Cayman Islands	Grand Cayman
Americas and Overseas Territories	Turks and Caicos Islands	Grand Turk
Americas and Overseas Territories	Mexico	Guadalajara
Indo-Pacific	China	Guangzhou
Americas and Overseas Territories	Guatemala	Guatemala City
Americas and Overseas Territories	Bermuda	Hamilton
Indo-Pacific	Vietnam	Hanoi
Africa	Zimbabwe	Harare
Africa	Somalia	Hargeisa
Americas and Overseas Territories	Cuba	Havana
Europe	Finland	Helsinki
Europe	Greece	Heraklion, Crete
Indo-Pacific	Vietnam	Ho Chi Minh City
Indo-Pacific	China	Hong Kong

Indo-Pacific	Solomon Islands	Honiara
Americas and Overseas Territories	United States of America	Houston
Indo-Pacific	India	Hyderabad
Europe	Spain	Ibiza
MENA & AfPak	Pakistan	Islamabad
Europe	Turkey	Istanbul
Europe	Turkey	Izmir

Indo-Pacific	Indonesia	Jakarta
Multilateral	Indonesia	Jakarta (ASEAN)
MENA & AfPak	Saudi Arabia	Jeddah
MENA & AfPak	Occupied Palestinian Territories	Jerusalem
Africa	South Africa	Johannesburg
Africa	South Sudan	Juba
MENA & AfPak	Afghanistan	Kabul (Afghanistan Office in Doha)
Africa	Nigeria	Kaduna (temporarily suspended)
Africa	Uganda	Kampala
Africa	Nigeria	Kano
MENA & AfPak	Pakistan	Karachi
Indo-Pacific	Nepal	Kathmandu
Africa	Sudan	Khartoum (currently closed)
Africa	Rwanda	Kigali
Americas and Overseas Territories	Jamaica	Kingston
Americas and Overseas Territories	Saint Vincent and the Grenadines	Kingstown
Africa	Democratic Republic of the Congo	Kinshasa
Indo-Pacific	India	Kolkata
Indo-Pacific	Malaysia	Kuala Lumpur
MENA & AfPak	Kuwait	Kuwait
Eastern Europe & Central Asia	Ukraine	Kyiv
Americas and Overseas Territories	Bolivia	La Paz
Africa	Nigeria	Lagos

MENA & AfPak	Pakistan	Lahore
Europe	Spain	Las Palmas
Africa	Malawi	Lilongwe
Americas and Overseas Territories	Peru	Lima
Europe	Portugal	Lisbon
Europe	Slovenia	Ljubljana
Americas and Overseas Territories	United States of America	Los Angeles
Africa	Angola	Luanda
Africa	Zambia	Lusaka

Europe	Luxembourg	Luxembourg
Europe	France	Lyon
Europe	Spain	Madrid
Europe	Spain	Malaga
Indo-Pacific	Maldives	Male
MENA & AfPak	Bahrain	Manama
Indo-Pacific	Philippines	Manila
Africa	Mozambique	Maputo
Europe	Turkey	Marmaris
Europe	France	Marseille
Africa	Lesotho	Maseru
Africa	Eswatini	Mbabane
Indo-Pacific	Australia	Melbourne
Americas and Overseas Territories	Mexico	Mexico City
Americas and Overseas Territories	United States of America	Miami
Europe	Italy	Milan
Americas and Overseas Territories	United States of America	Minneapolis
Eastern Europe & Central Asia	Belarus	Minsk
Africa	Somalia	Mogadishu
Africa	Liberia	Monrovia
Americas and Overseas Territories	Mexico	Monterrey

Americas and Overseas Territories	Uruguay	Montevideo
Americas and Overseas Territories	Canada	Montreal
Americas and Overseas Territories	Montserrat	Montserrat (Plymouth)
Eastern Europe & Central Asia	Russia	Moscow
Indo-Pacific	India	Mumbai
Europe	Germany	Munich
MENA & AfPak	Oman	Muscat
Africa	Kenya	Nairobi

Americas and Overseas Territories	Bahamas	Nassau
Africa	Chad	N'Djamena
Indo-Pacific	India	New Delhi
Americas and Overseas Territories	United States of America	New York CG
Multilateral	United States of America	New York UKMIS
Africa	Niger	Niamey
Europe	Cyprus	Nicosia
Africa	Mauritania	Nouakchott
Indo-Pacific	Tonga	Nuku'alofa
Americas and Overseas Territories	United States of America	Orlando
Indo-Pacific	Japan	Osaka
Europe	Norway	Oslo
Americas and Overseas Territories	Canada	Ottawa
Europe	Spain	Palma
Americas and Overseas Territories	Panama	Panama City
Europe	France	Paris Embassy
Multilateral	France	Paris OECD
Indo-Pacific	Australia	Perth

Indo-Pacific	Cambodia	Phnom Penh
Europe	Montenegro	Podgorica
Americas and Overseas Territories	Haiti	Port au Prince
Africa	Nigeria	Port Harcourt
Africa	Mauritius	Port Louis
Indo-Pacific	Papua New Guinea	Port Moresby
Americas and Overseas Territories	Trinidad and Tobago	Port of Spain
Americas and Overseas Territories	Falkland Islands	Port Stanley
Indo-Pacific	Vanuatu	Port Vila
Europe	Portugal	Portimao
Europe	Czech Republic	Prague

Africa	South Africa	Pretoria
Europe	Kosovo	Pristina
Indo-Pacific	India	Pune
Indo-Pacific	Democratic People's Republic of Korea	Pyongyang (closed)
Americas and Overseas Territories	Ecuador	Quito
MENA & AfPak	Morocco	Rabat
Americas and Overseas Territories	United States of America	Raleigh
Americas and Overseas Territories	Brazil	Recife
Europe	Iceland	Reykjavik
Europe	Greece	Rhodes
Europe	Latvia	Riga
Americas and Overseas Territories	Brazil	Rio de Janeiro
MENA & AfPak	Saudi Arabia	Riyadh
Europe	Italy	Rome

Americas and Overseas Territories	United States of America	San Diego
Americas and Overseas Territories	United States of America	San Francisco
Americas and Overseas Territories	Costa Rica	San Jose
Americas and Overseas Territories	El Salvador	San Salvador
MENA & AfPak	Yemen	Sana'a (Yemen Office Riyadh and Amman)
Europe	Spain	Santa Cruz de Tenerife
Americas and Overseas Territories	Chile	Santiago
Americas and Overseas Territories	Dominican Republic	Santo Domingo
Americas and Overseas Territories	Brazil	Sao Paulo
Europe	Bosnia	Sarajevo

Americas and Overseas Territories	United States of America	Seattle
Indo-Pacific	South Korea	Seoul
Indo-Pacific	China	Shanghai
Indo-Pacific	Singapore	Singapore
Europe	North Macedonia	Skopje
Europe	Bulgaria	Sofia
Europe	Croatia	Split
Americas and Overseas Territories	Grenada	St George's
Americas and Overseas Territories	Saint Helena	St Helena
Americas and Overseas Territories	Antigua and Barbuda	St John's
Europe	Sweden	Stockholm
Multilateral	France	Strasbourg

Indo-Pacific	Fiji	Suva
Indo-Pacific	Australia	Sydney
Indo-Pacific	Taiwan	Taipei
Europe	Estonia	Tallinn
Eastern Europe & Central Asia	Uzbekistan	Tashkent
Eastern Europe & Central Asia	Georgia	Tbilisi
MENA & AfPak	Iran	Tehran
MENA & AfPak	Israel	Tel Aviv
Europe	Netherlands	The Hague
Americas and Overseas Territories	Anguilla	The Valley
Europe	Albania	Tirana
Indo-Pacific	Japan	Tokyo
Americas and Overseas Territories	Canada	Toronto
Americas and Overseas Territories	British Virgin Islands	Tortola
MENA & AfPak	Libya	Tripoli
Americas and Overseas Territories	Tristan da Cunha	Tristan da Cunha
MENA & AfPak	Tunisia	Tunis
Multilateral	Italy	UK Permanent Representation to the United Nations Agencies for Food and Agriculture, Rome
Indo-Pacific	Mongolia	Ulaanbaatar
Europe	Malta	Valletta
Americas and Overseas Territories	Canada	Vancouver
Europe	Holy See	Vatican City
Africa	Seychelles	Victoria
Europe	Austria	Vienna
Multilateral	Austria	Vienna UKDEL
Multilateral	Austria	Vienna UKMIS
Indo-Pacific	Laos	Vientiane
Europe	Lithuania	Vilnius
Europe	Poland	Warsaw

Americas and Overseas Territories	United States of America	Washington DC
Indo-Pacific	New Zealand	Wellington
Africa	Namibia	Windhoek
Indo-Pacific	China	Wuhan
Indo-Pacific	Myanmar (Burma)	Yangon
Africa	Cameroon	Yaounde
Eastern Europe & Central Asia	Russia	Yekaterinburg
Eastern Europe & Central Asia	Armenia	Yerevan
Europe	Croatia	Zagreb
Europe	Greece	Zakynthos

## 19. ANNEX 2 – PARTNERS ACROSS GOVERNMENT ON THE ONE HMG OVERSEAS PLATFORM

<b>One HMG Partner:</b>
Foreign, Commonwealth & Development Office
Bank of England
British Council
British Tourist Authority (trading as Visit Britain/Visit England)
Cabinet Office, including: - GCSI - Government Communication Service International - GDS: Government Digital Service
Centre for Environment, Fisheries & Aquaculture Science (CEFAS)
Crown Prosecution Service
Department for Business, Energy and Industrial Strategy*
Department for Digital Culture Media and Sport
Department for Environment Food and Rural Affairs (DEFRA)
Department of Health & Social Care
Department for International Trade
Department for Transport, including: - Maritime and Coastguard Agency
Department of Work and Pensions
Financial Conduct Authority
Food Standards Agency
Her Majesty's Revenue and Customs
HM Treasury



Home Office, including: - HM Passport Office - Home Office International - Home Office – International Operations [replaces BFI & IEI] - Return Logistics Operations - Homeland Security Groups - UK Visas & Immigration
Intellectual Property Office
Manchester City Council
Medicines and Healthcare Products Regulatory Agency
Meteorological Office
Metropolitan Police
Ministry of Defence, including: - British Defence Section Washington - Defence Attaché Network - Defence Geographic Centre - UK Hydrographic Office
National Crime Agency
Office for National Statistics
Oil Pipeline Agency
UK Health Security Agency
UK Intelligence Community
UK Research & Innovation

<b>Devolved Governments:</b>
Invest Northern Ireland
The Executive Office, Northern Ireland
Scottish Enterprise, including: - Scottish Development International
Scottish Government
Welsh Government, including: - International Business Wales

\*Department for Business, Energy and Industrial Strategy existed until 2023 when it was split to form the Department for Business and Trade (DBT), the Department for Energy Security and Net Zero (DESNZ) and the Department for Science, Innovation and Technology (DSIT). Responsibility for national security and investment policy has gone to the Cabinet Office.

## 20. ANNEX 3 – CURRENT/HISTORIC METHODOLOGIES FOR CALCULATING COST OF LIVING ALLOWANCES AND HARDSHIP ALLOWANCES

### Current/historic methodology for calculating Cost of Living Allowances (COLA)

Currently the FCDO undertakes a worldwide costing exercise in March each year which is then updated in September. This exercise takes a number of weeks to collate, check and distribute the information. The data gathered is used to calculate the Cost of Living Allowance (COLA) that the FCDO provides to its staff serving overseas. The FCDO has approximately 17,500 people in over 280 diplomatic offices, operating in over 170 countries.

COLA rates are susceptible to regular change. Factors that can affect COLA rates include, but are not limited to:

- A new cost of living index calculated by the service provider ( the requirement)
- Changes in salary
- Changes in rates of inflation at Post
- Changes in exchange rates
- Price changes in the UK
- The annual UK Living Costs and Food Survey (LFS) exercise

Revised FCDO indices are currently produced in July and January of the following year, using the latest exchange rates and adjusting inflation as necessary. The exchange rate for converting local currency is taken from OANDA. In high inflation countries, or in exceptional circumstances COLA revisions need to be conducted more frequently. For example if the base rate of exchange used to calculate COLA, changes by 10% for two consecutive months, this triggers a revision of COLA rates. If the rate of inflation fluctuates by 10% over a sustained period of 8 weeks a revision of COLA rates in that country will be triggered.

We would expect the supplier to monitor inflation and exchange rates, as well as any other factors affecting COLA and flag to the Authority when a COLA revision might be necessary.

Currently the system for calculating COLA is based on working out the percentage difference between the cost of living in the UK and that at Posts overseas. This is done by comparing the London cost of a basket of goods and services items (considered to be widely available globally) with the equivalent items at all locations. These items have been chosen to produce a consistent standard of comparability worldwide. Through this exercise an index is produced for each post. London would be considered 100 so an index of 120 indicates that the cost of living is 20% higher than London. Or an index of 95 indicates that the cost of living is 5% lower than London. There is no negative scoring so any index indicating a lower than London score would be zero-rated.

The index is then applied to the proportion of the officer's salary (Home Spendable Income), which covers everyday expenses to produce the COLA uplift.

In addition to the basic COLA, assignment costs are added. Assignment costs include:

- Children: childcare
- Recreation: Access to a wide range of leisure facilities (especially public swimming pools, golf courses, tennis courts etc.) is not universally available overseas. To compensate for the consequential additional costs of recreational pursuits, a sum of money will need to be generated by the supplier on the basis of the average annual fees of up to five clubs used by expatriates in those cities.
- International Telephone calls: The local cost of 60 and 45 minutes of international calls.

Full details of all assignment costs are provided by the Authority.

Currently FCDO employees are given the opportunity to provide details and commentary on their shopping habits including shops, price, and brands through a supplier survey (twice annually). A costing survey is provided for all staff to complete and send back to the supplier including a variety of items from the following categories: groceries, dairy produce, meat and fish, fresh fruit and vegetables, household goods, drink and tobacco, electrical goods, recreational goods, services, motoring, meals and drinks out. A separate survey (twice annually) also allows FCDO employees to provide information on their environment and living conditions including comments on the costs of joining sports and social clubs and the cost of domestic staff. Such participation facilitates engagement and buy in from staff who can inform, but not improperly influence those collecting the data.

#### Current/historic methodology for calculating Hardship Allowances

A Hardship allowance is paid to compensate staff and their families for the additional costs of maintaining quality of life at hardship Posts. Examples of how this allowance is used include:

- Taking additional breaks from the country (transport, accommodation etc)
- Security issues to manage including requirement for security devices
- The need for specialist four wheel drive vehicles
- Loss or damage to private property, cars etc due to violence or burglaries
- Additional insurance requirements, including life assurance premiums
- Extra maintenance of vehicles where driving conditions/servicing are poor
- Preventative health measures and medicines
- Damage to electrical equipment by fluctuating currents; provision of voltage regulators etc

The Hardship allowance also provides compensation for the wider challenges that officers face in locations globally when compared to life in the UK and working in London.

Currently each Post has an individual score in relation to hardship. Many do not receive the qualifying level for this allowance to be paid. The rate of payment is based on the number of points gained by each individual Post. Any Post scoring above a qualifying mark receives the allowance. No predetermined limit is set on the number of qualifying Posts. A complete list of all current FCDO Posts along with whether they are currently classified as Hardship Posts can be found in **ANNEX 1 – FULL LIST OF FCDO POSTS**. Please note: A Post's hardship status can change regularly.

Individual rates are then based on a combination of two scores:

- 1) Hardship scoring system (the requirement): this makes up the bulk of total points for each location and is generated from expatriates and independent sources. These scores reflect the particular relevance of factors in the areas of natural phenomenon, air pollution, language, culture, goods & services, external isolation, news & media, recreation, housing, utilities, education, personal security and socio-political tensions.
- 2) A security score provided by FCDO's Estates Security and Network Directorate (ESND): this is a smaller additional score reflecting increased security threats to FCDO/HMG staff, over and above the private sector employees, relating to terrorism and hostile intelligence. ESND conducts an annual survey, which assesses reporting from Posts and analyses from official sources.

Currently rates are reviewed annually on 1 February.

The current Hardship Survey is aimed at UK-based staff, as potential recipients of Hardship allowance and therefore ideally any survey should be completed by a member of UK Based (UKB) staff or UKB family member. Currently it is completed as an online questionnaire which gathers observations of life at Post.

Current/historic service requirements:

Services must continue to evolve to meet the needs of an increasingly diverse mobile workforce, and ever-changing global environment and also the potential for any policy changes by the authority to reflect any changes in working practices or conditions. The provider will need to be flexible to accommodate the opening of new FCDO Posts across the world and the need for ad hoc data collection for these Posts. This would include Post data being required outside the normal data collecting period although it is expected that at least 8 weeks' notice should be given. We would not expect this to be more than 4 additional Posts in any given year.

Current/historic data collection/presentation requirements:

Data should be collected from multiple primary sources, ensuring its reliability and accuracy. Data calculations undertaken on behalf of the FCDO should ensure that FCDO assumptions and rules are consistently applied to every location.

A team of researchers should collate the data, supported by knowledge of each location's commercial, retail and political environment from assignees who live and work in each location. This ensures the data provided remains relevant as the location's landscape changes.

Published data should be tailored to meet specific FCDO requirements that take into account the scope of FCDO's international presence and unique workforce needs. Datasets should be designed in consultation with the FCDO to account for these needs and the specific uses for the data ensuring consistency in the FCDO's ability to provide accurate and timely allowances to their staff serving overseas.

The supplier should provide detailed explanations of why, when and how a figure has changed, putting the complexities of economic conditions into a simple explanation as to why an employee's allowance has changed.

## 21. APPENDICES

## 22.1 APPENDIX 1 – AUTHORITY CYBER SECURITY REQUIREMENTS

## Authority Security Requirements

		Schedule Applicability			
1.Information Security Risk Management		Extended	Developer	Consultancy/ Professional Services	Lit e
Approach to Risk Management	1.1 The Supplier shall operate and maintain policies and processes for risk management in line with the Information Security Risk Management Policy, during the Contract Period, which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that The Authority Security Requirements are met.	✓	✓	✓	✓
	1.2 The Supplier shall provide their Risk Management Policy to the Authority upon request within 10 Working Days of such request. Working collaboratively, the Authority may request changes to ensure compliance with the Authority Security Requirements and where necessary to meet Authority risk appetite.	✓	✓	✓	✓
	1.3 Where the Authority deems it necessary, the Supplier may be required to implement changes within one calendar month or on a date that has been mutually agreeable by both parties.	✓	✓	✓	✓
Risk Identification and Management throughout delivery of service	1.4 The Supplier shall be responsible for the identification of security risks, which shall be recorded within a risk register on identification. The risk register will be shared with the Authority as agreed and to be reviewed at an appropriate governance forum where applicable.	✓	✓	✓	
	1.5 The Supplier shall provide the report of the Risk Assessment to the Authority, in the case of at least annual Risk Assessments, within 10 working days of the risk assessment report being delivered to the Supplier, it shall share said report with the Authority, in a redacted form if necessary.	✓	✓	✓	
	1.6 The Supplier shall be responsible for delivering Risk Management continuously throughout delivery stage of the service.	✓	✓	✓	✓
	1.7 The Supplier shall notify the Authority within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.	✓	✓	✓	✓
	1.8 Following the collaborative review of the output from a risk assessment, should the	✓	✓	✓	

	Authority require the application of additional controls to address High or Medium findings, the Authority can request a further risk assessment be completed within one calendar month.				
<b>2. Organisation of Information Security</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Supplier Roles and Responsibilities</b>	2.1 The Supplier will employ a Role Base Access Control Model (RBAC) covering Supplier roles, this will include the role, associated responsibilities and the technical accesses granted for all IT supporting the service.	✓	✓	✓	✓
	2.2 The Supplier will ensure that a suitably qualified and experience person (SQEP) is employed to provide expertise and recommendations to Suppliers in all projects and programs unless otherwise instructed by the Authority.	✓	✓	✓	
<b>Contact with Authorities</b>	2.3 The Supplier shall apply a principle of least privilege to all roles directly and indirectly supporting the service, ensuring that no one individual has inflated or excessive privileges.	✓	✓	✓	✓
<b>3. Human Resources</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Pre-Employment Checks</b>	3.1 The Supplier shall have a documented policy and or process regarding employment of staff, which must include as a minimum, a pre-employment check, which are required under the HMG Baseline Personnel Security Standard which includes: <ul style="list-style-type: none"> <li>• Verification of the individual's identity.</li> <li>• Verification of the individual's nationality and immigration status.</li> <li>• Verification of the individual's employment history.</li> <li>• Verification of the individual's criminal record.</li> </ul>	✓	✓	✓	
<b>Management of Clearances, Changes to Details</b>	3.2 The Supplier shall ensure all Supplier's staff supporting the delivery of the services on the Authority premises have a valid Security Check (SC) or Developed Vetting (DV) clearance level and comply with Authority's onboarding requirements and supporting requirements.	✓	✓	✓	✓
	3.3 The Supplier will ensure that a managed Joiners Movers Leavers process is in operation and is viewable upon request by the Authority.	✓	✓	✓	
<b>Vetting</b>	3.4 The Authority and the Supplier shall review the roles and responsibilities of the Supplier Staff involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (e.g., a Counter Terrorist Check; a Security Check).	✓	✓	✓	✓

	3.5 The Supplier shall not permit Supplier Staff who fail the security checks required, to be involved in the management and/or provision of the Services, except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.	✓	✓	✓	✓
<b>Access to Authority Data</b>	3.6 The Supplier shall ensure that Supplier Staff are only granted access to Authority Data as is necessary to enable the Supplier Staff to perform their role and to fulfil their responsibilities.	✓	✓	✓	✓
	3.7 The Supplier shall ensure that Supplier Staff who are no longer supporting the engagement are off boarded and associated access to Authority data is revoked immediately.	✓	✓	✓	
<b>Access to Estate, IT Infrastructure</b>	3.8 The Supplier shall ensure that Supplier Staff who have access to the Authority's sites, the IT Environment or The Authority Data have received security training via onboarding process.	✓	✓	✓	✓
<b>Security Training (Personal data)</b>	3.9 The Supplier shall provide their staff with appropriate ongoing support and cyber security training to help them manage personal data securely, including the technology they use in line with Industry best practice.	✓	✓	✓	✓
	3.10 The Supplier shall ensure, at a minimum, that the training provided to Supplier Staff includes: <ul style="list-style-type: none"> <li>• Training on the identification and reporting fraudulent communications intended to induce individuals to disclose</li> <li>• Personal data or any other information that could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Sites, the IT Environment or The Authority Data ("phishing").</li> </ul>	✓	✓	✓	✓
<b>4 Information Security Management System (ISMS)</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Governance</b>	4.1 The supplier shall have a documented Information Security (IS) Policy in place that must: <ul style="list-style-type: none"> <li>• Undergo a fit for purpose review at least annually</li> <li>• States compliance with the Security Policy is mandatory for all colleagues</li> <li>• Include information security roles &amp; responsibilities</li> <li>• Identify roles and responsibilities of individuals / teams within each function, e.g. org chart</li> </ul>	✓	✓	✓	✓



	<ul style="list-style-type: none"> <li>Be agreed / signed-off by management</li> </ul>				
<b>Legal and Regulatory Compliance</b>	<p>4.2 The supplier shall demonstrate they can manage compliance and understanding of Legal (e.g. GDPR and Network and Information Systems Regulation (NIS)) and regulatory requirements regarding cyber security, including privacy obligations:</p> <ul style="list-style-type: none"> <li>Changes to the regulatory requirements in relevant jurisdictions must be monitored</li> <li>Security program / controls must be updated to reflect changes</li> <li>Relevant legal / regulatory requirements must be complied with</li> </ul>	✓	✓	✓	✓
<b>Scope</b>	<p>4.3 The Supplier and the Authority must demonstrate that the scope of the service is understood. The following must be documented:</p> <ul style="list-style-type: none"> <li>What Authority data is within scope of the engagement.</li> <li>Where it is stored / hosted, processed and transmitted</li> <li>Who has access to it including onward transmission to third parties which will require explicit approval from Authority security Department.</li> <li>Controls to protect Confidentiality, Integrity and Availability.</li> <li>Data flow mapped, to include all systems used to provide the service.</li> </ul>	✓	✓	✓	✓
<b>Reporting</b>	<p>4.4 The Supplier shall have a ISMS compliance management and assessment process in place which includes the following:</p> <ul style="list-style-type: none"> <li>Methods to test compliance to controls within the ISMS</li> <li>Reporting of compliance and non-compliance to management</li> <li>A governance framework in place with appropriate escalation</li> <li>Agreeing exceptions to policy • Identification and update on threats.</li> </ul>	✓	✓	✓	✓
<b>Information Security Management System</b>	<p>4.5 The Supplier shall design the Core Information Management System as amended from time to time in accordance with:</p> <ul style="list-style-type: none"> <li>The NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <a href="https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main">https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main</a>;</li> <li>the NCSC "Bulk Data Principles", a copy of which can be found at: <a href="https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main">https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main</a>; and</li> <li>The NCSC "Cloud Security Principles", a copy of which can be found at:</li> </ul>	✓	✓	✓	✓



	<a href="https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles">https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles</a>				
<b>5 Asset Management</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Inventory</b>	5.1 The Supplier shall maintain an asset inventory with all assets used by the Supplier and sub-contractors. The asset inventory shall include all assets the Supplier has access to including hardware, software, firmware, peripheral devices and removable media.	✓	✓	✓	✓
	5.2 The Supplier shall provide the Authority with access to asset inventory reports, to ensure all assets are accounted for across the entire asset lifecycle.	✓	✓	✓	✓
	5.3 The Supplier shall maintain a record of what data is stored and where the data is stored and processed, including back-ups, local cache, and downloads.	✓	✓	✓	✓
<b>Asset Owners</b>	5.4 The Supplier shall maintain a record of the personnel responsible for the security of data assets (i.e. Data Owner or Information Asset Owner).	✓	✓	✓	
	5.5 The Supplier shall evidence an Asset and Configuration Management Policy or equivalent.	✓	✓	✓	
	5.6 The Supplier shall provide the Authority with access to the record of personnel responsible for security of the data assets.	✓	✓	✓	
<b>Acceptable Use of Assets</b>	5.7 The Supplier shall comply with the Authority's acceptable use policy.	✓	✓	✓	✓
	5.8 Where the Supplier shall be issued with a corporate device for conducting business, personal laptops and Supplier corporate laptops are not to be used for managing and delivering the service unless necessary and unless agreed in writing by the Authority .	✓	✓	✓	
	5.9 The Supplier shall ensure that physical media is protected during transportation and to be sealed with a padlock and one-time use security seal. Cases should have a case strap with combination lock, use constrictor technology and tamper indicators. Transportation of physical media should use point-to-point courier services, and should be trackable in real time with anti-bandit locks. Delivery should be arranged beforehand with specific day/time and proof of delivery, and processes must be put in place to provide the Authority with a notification of failed delivery or suspicion that the media has been tampered with.	✓	✓	✓	✓
<b>Return of Assets</b>	5.10 The Supplier shall ensure that all assets are tracked and returned to the Authority and in accordance with the agreed exit plan.	✓	✓	✓	

<b>Data Destruction</b>	5.11 The Supplier shall ensure that Physical Data (including hard copy data, non-reusable storage media, stamped plastic note bags, laminated paper, and credit/debit cards) is disposed of in confidential waste bins.	✓	✓	✓	
<b>6 Access Management</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/Professional Services</b>	<b>Lit e</b>
<b>Identity and Access Management Policies, Process</b>	6.1 The Supplier shall develop and maintain appropriate identity and access management policies and processes which covers who should have access to which systems, data or functionality, why, and under what circumstances.	✓	✓	✓	✓
	6.2 The Supplier shall take into consideration all potential types of users including full and part-time staff, sub-contractors, contractors as part of the identity and access management policies and process.	✓	✓	✓	✓
<b>Access Control Regime</b>	6.3 The Supplier shall operate an access control regime to ensure: <ul style="list-style-type: none"> <li>All users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services;</li> <li>And all persons who access the sites are identified and authenticated before they are allowed access to the sites.</li> </ul>	✓	✓	✓	✓
<b>User Registration: Unique IDs</b>	6.4 The Supplier shall ensure that all new user IDs for network or application accounts are linked to a unique individual.	✓	✓	✓	✓
	6.5 The Supplier shall ensure all access permissions are defined and documented at the Entitlement Level.	✓	✓	✓	
	6.6 The Supplier shall ensure that any service accounts or shared accounts are linked to a unique identity and are tied to an appropriate business justification and approvals. Approvals for such accounts must also be appropriately segregated from those using the account and be subject to ongoing independent review and monitoring.	✓	✓	✓	
<b>Multi Factor Authentication (MFA) and Password Authentication</b>	6.7 The Supplier shall have an industry aligned password policy in place to authenticate users to the network, applications, and devices. The Supplier's password policy must require all default passwords to be changed and must remove or suspend unused accounts.	✓	✓	✓	✓
	6.8 The Supplier shall consider the use of multi-factor authentication for all user accounts relating to the service that are either privileged or are internet facing web services.	✓	✓	✓	✓
<b>User Access Provisioning</b>	6.9 The Supplier shall ensure access requests are reviewed and authorised by appropriate	✓	✓	✓	✓

	individuals and cannot be raised and approved by the same user.				
	6.10 The Supplier shall ensure that approval requirements for access requests are determined on the basis of risk.	✓	✓	✓	✓
<b>Privileged Access</b>	6.11 The Supplier shall use a tiered model for administrative accounts and only use accounts with full privileges (i.e. Domain admin, global admin, or cloud admin accounts) when necessary and with best practice controls applied accordingly.	✓	✓	✓	✓
<b>Excessive Access Rights</b>	6.12 The Supplier shall apply a principle of segregation of duties to all roles directly and indirectly supporting the service, ensuring that no one individual has excessive access rights.	✓	✓	✓	✓
	6.13 The Supplier shall apply a principle of least privilege to all roles directly and indirectly supporting the service, ensuring that no one individual has inflated or excessive privileges.	✓	✓	✓	✓
<b>Management of Privileged Access Rights</b>	6.14 The Supplier shall ensure that Privileged access rights comply with the following; <ul style="list-style-type: none"> <li>• The user account will only have access as specified in the jointly approved RBAC model.</li> <li>• Any change to the access will be encompassed within an authorisation process.</li> <li>• In relation to an Admin account; <ul style="list-style-type: none"> <li>- The account must be separate to the users standard account.</li> <li>- The account must only be used for admin specific tasks and not for daily use.</li> <li>- There must be no internet access from the admin account.</li> <li>- The admin account will be restricted to ensure it meets the business requirement.</li> <li>- The account must be requested through an approved process that is agreed with the Authority.</li> </ul> </li> </ul>	✓	✓	✓	
<b>Segregation of Duties (SoD)</b>	6.15 The Supplier shall ensure access is granted, aligned with a defined a segregation of duties (SoD) matrix where toxic combinations duties have been identified.	✓	✓	✓	
	6.16 The Supplier shall ensure SoD conflicts are prevented where possible when provisioning access to roles. Where it is not possible to remediate violations, a formal risk acceptance or dispensation process must be in place to define compensating controls and manage the risk.	✓	✓	✓	
<b>Protection of Authentication Information</b>	6.17 The Supplier shall ensure that the generation and distribution of authentication information is performed in a secure manner. Where default passwords are allocated,	✓	✓	✓	✓

	passwords / PINs must be changed upon first successful authentication by the user.				
	6.18 The Supplier shall ensure that requests for the resetting of authentication must be confirmed as coming from the identified owner or a delegate. Compromised or suspected compromised authentication information must be promptly changed.	✓	✓	✓	✓
	6.19 The Supplier shall ensure that passwords are stored using one-way encryption (e.g. hashing).	✓	✓	✓	
<b>Review of Access Rights</b>	6.20 The Supplier shall regularly review access rights. If an employee changes role or leaves the organisation, existing access must be reviewed, and any access no longer required is removed immediately.	✓	✓	✓	✓
	6.21 The Supplier shall generate an Access Control lists (also called user access lists) for all relevant applications and networks, detailing the up-to-date and accurate access rights of relevant users from a reliable source.	✓	✓	✓	
	6.22 The Supplier shall ensure that network and application accounts are recertified on a regular basis (e.g. quarterly) based on the risk associated to the access (e.g. privileged access or financial control access). Following recertification, applicable updates to user access must be made and evidence of the activity retained.	✓	✓	✓	
	6.23 The Supplier shall ensure that Entitlements underlying roles are reviewed on a longer-term review cycle, (e.g. annually) to ensure they are appropriate for the role being provisioned to users.	✓	✓	✓	
<b>Removal/ Adjustment of Access Rights</b>	6.24 The Supplier shall have a policy or process which addresses the below requirements; <ul style="list-style-type: none"> <li>Revocation of leaver within 24 hours / 1 working day.</li> <li>Processes for the emergency revocation of accounts/access.</li> <li>For dormant accounts</li> <li>on the last day of service for high risk systems (e.g. AD, VPN, DMS);</li> <li>not more than 5 business days following a user leaving or the account is no longer required to provide the service.</li> </ul>	✓	✓	✓	
	6.25 The Supplier shall ensure Access Rights logs are maintained to include the following: <ul style="list-style-type: none"> <li>when removal of access was requested and by whom:</li> <li>date &amp; time user left; and</li> <li>date &amp; time account was revoked</li> </ul>	✓	✓	✓	✓
<b>Code of Conduct</b>	6.26 The Supplier shall complete and submit to the Authority a Code of Connection (CoCo) document in preparation for all	✓	✓	✓	

<b>(CoCos) and Rules of Engagement</b>	connectivity to Authority IT systems or networks as part of the service provision.				
	6.27 The Supplier shall ensure that the Code of Connection document is aligned to agreements in the Security Management Plan, and should contain the rules of engagement for managing escalations, performance or security incidents and how “connectivity” risk should be managed and communicated to the Authority for the duration of the connection.	✓	✓	✓	
	6.28 The Supplier shall use the Code of Connection template as provided by the Authority, to record a formal agreement between the Supplier and the Authority on security measures to be applied by the 3rd party prior to, and during any electronic connection with an Authority IT system or network.	✓	✓	✓	
	6.29 The Supplier must not establish a connection with the Authority live operational IT systems or Networks without prior written approval.	✓	✓	✓	
<b>7 Information Classification</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Process of Authority Data</b>	<p>7.1 If the provision of the services requires the Supplier to Process Authority Data which is classified as:</p> <ul style="list-style-type: none"> <li>OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with The Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.</li> </ul>	✓	✓	✓	✓
<b>Personal Data</b>	7.2 The Supplier shall not keep personnel data for no longer than a time period to be agreed with the Authority.	✓	✓	✓	✓
	7.3 Where the Supplier is identified as a GDPR Data Processor, all provision under GDPR are applied.	✓	✓	✓	✓
	7.4 The Supplier shall understand, document and manage access to personal data and systems that process Authority data. Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed.	✓	✓	✓	✓
	7.5 The Supplier shall undertake activities to check or validate that the technical system permissions are consistent with the documented user access rights.	✓	✓	✓	✓

<b>Handling of data</b>	7.6 The Supplier shall have a policy that meets or exceeds for the re-use, repair, disposal and destruction of storage media and any devices that could store data, (including office equipment such as printers and photocopiers, monitors and TVs).	✓	✓	✓	✓
<b>Data Integrity</b>	7.7 The Supplier shall ensure that controls are in place at the point of origin and receipt of data to verify properties of the data such as the number of records, to prevent records from being accidentally replicated, or the dataset as whole being duplicated.	✓	✓	✓	✓
	7.8 The Supplier shall ensure that mechanisms are in place to restore or re-source data suspected of being corrupted or inaccurate.	✓	✓	✓	✓
	7.9 The Supplier shall ensure that sampling is performed against source records at the point of receipt, and whilst at rest, to validate the accuracy of the data and identify data corruption.	✓	✓	✓	✓
<b>Disposal of Data</b>	7.10 The Supplier shall, prior to disposal of Authority data, ensure all labels or markings that indicate ownership of the device (or the nature of the data contained) are removed. If using trusted third parties for destruction hold them to recognised standards and obtain destruction certificates.	✓	✓	✓	
<b>Sanitisation of Data</b>	7.11 The Supplier shall periodically verify that the Authority data is being sanitised appropriately, and test destruction processes and equipment.	✓	✓	✓	
<b>Process of Data</b>	7.12 The Supplier shall not process Authority data outside of the UK without the prior written consent of the Authority, which may be subject to conditions.	✓	✓	✓	✓
<b>Data Records</b>	7.13 The Supplier shall maintain data records of data processing activities and have appointed a Data Protection Officer (DPO). In the absence of a DPO, the Supplier must provide a named individual with ultimate responsibility for data protection in the Supplier's organisation.	✓	✓	✓	✓
	7.14 The Supplier shall track and document the Authority's personal data processes and provide a description for the purpose of process.	✓	✓	✓	✓
<b>Data Privacy Impact Assessment</b>	7.15 The Supplier shall undertake a Data Privacy Impact Assessment to ascertain the level of impact to data subjects prior to commencement of the service. This should be submitted to the ODPO for approval and periodic review.	✓	✓	✓	
<b>Compliance</b>	7.16 The Supplier shall take steps to assess data protection and GDPR / UK Data Law risks.	✓	✓	✓	✓
	7.17 The Supplier shall collaborate with the Office of the Data Protection Officer to work towards and maintain compliance with UK	✓	✓	✓	✓

	data legislation and data protection requirements.				
	<p>7.18 The Supplier shall include appropriate organisation measures to make effective risk-based decisions upon:</p> <ul style="list-style-type: none"> <li>• The state of the art [of technology]</li> <li>• Cost of implementation</li> <li>• The nature, scope, context and purpose of processing', and</li> <li>• The severity and likelihood of the risk being realised.</li> </ul>	✓	✓	✓	✓
<b>8 Cryptography</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Encryption</b>	8.1 The Supplier shall meet NCSC data in transit and data at rest protection requirements through a combination of encryption, network protection and authentication as recommended by the NCSC.	✓	✓	✓	✓
	8.2 Unless otherwise stated by the Authority, the Supplier shall be responsible for encryption and its implementation, key material and key management used to protect Authority data in transit.	✓	✓	✓	✓
	8.3 Unless otherwise agreed the Supplier shall be responsible for defining key management processes for all aspects of the key lifecycle, including key generation, storage, inventory, expiration, destruction, details of which shall be available upon request.	✓	✓	✓	✓
	8.4 The Supplier shall ensure that when used, keys are regularly rotated, and there are processes to manage key compromise events, details of which shall be available upon request.	✓	✓	✓	✓
	8.5 The Supplier shall ensure that all data flows between the Authority and the Supplier are encrypted. Encryption must be between all endpoints and components of the service and will employ cryptographic standards and ciphers as recommended by NCSC.	✓	✓	✓	✓
	8.6 The Authority and Supplier shall both be authenticated, but method does not require to be the same for both parties.	✓	✓	✓	✓
	8.7 The Supplier shall ensure all network layer protections should include encryption between endpoints and components of the service, configured according to the latest NCSC and recommendations.	✓	✓	✓	✓
	8.8 The Supplier shall encrypt all data that is transiting between data centers. This includes data flows initiated by the Authority application(s) and those initiated by the underlying service platform, including application data, database synchronization, backup remote storage and log aggregation	✓	✓	✓	✓
	8.9 The Supplier shall ensure that privacy between different customers of services which	✓	✓	✓	✓



	can be accessed via software defined private networks (SD-WAN), is implemented by a combination of routing protocols and encryption.				
<b>IPsec</b>	8.10 The Supplier shall ensure that software defined private networks (SD-WAN) implementations have options to encrypt traffic using IPsec. This encryption should include end-to-end protection and is configured using a good profile as described by IPsec guidance <a href="https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data">https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data</a> .	✓	✓	✓	✓
	8.11 The Supplier shall ensure that any services accessed via bonded fiber-optic connections, or private WAN circuits offered by a telecommunications providers are encrypted using TLS or IPsec and configured using a good profile. See NCSC IPsec and TLS guidance for details.	✓	✓	✓	✓
	8.12 The Supplier shall ensure, devices which implement cryptographic protection of information using IPsec should: <ul style="list-style-type: none"> <li>• be deployed and managed by a competent resource in a manner that does not undermine the protection they provide, from a suitable management platform.</li> <li>• be configured to provide effective cryptographic protection.</li> <li>• be disposed of securely.</li> <li>• generate and protect private keys in an appropriate manner.</li> <li>• be patched promptly upon release of updated software or firmware (implementation issues can introduce vulnerabilities that can be exploited if devices are left unpatched)</li> <li>• use certificates as a means of identifying and trusting other devices using a suitable PKI, possibly an in-house PKI (by exception Pre-Shared Keys (PSKs) may be used for authentication where certificates are not supported by both peers)</li> </ul>	✓	✓	✓	✓
<b>Data in Transit</b>	8.13 The Supplier shall provide confirmation in writing to the Authority that within the Supplier's service, the Authority data is protected in transit to NCSC or agreed standards.	✓	✓	✓	✓
	8.14 The Supplier shall track and inform the Authority, on every occasion, when the Authority data in transit is accessed via external interfaces. This includes where data is moved between physical data centers.	✓	✓	✓	✓
<b>Security Controls</b>	8.15 On request the Supplier shall inform the Authority how the security controls are enforced to protect data flows and data flow rules.	✓	✓	✓	✓



<b>Keys</b>	8.16 The Supplier shall not use Group Domain of Interpretation (GDOI), nor other approaches for establishing shared keys across multiple devices.	✓	✓	✓	✓
	8.17 The Supplier shall inform the Authority if there is an intent to use PSKs in site-to-site VPNs.	✓	✓	✓	✓
	8.18 If authorised by the Authority, the Supplier shall ensure PSKs are: <ul style="list-style-type: none"> <li>Generated in a cryptographically secure manner and have at least 128 bits of entropy.</li> <li>Unique to a group of devices that need to authenticate each other, and not shared across different groups.</li> <li>Handled securely and only by authorised personnel (from the point of creation, through distribution, to eventual destruction) to prevent compromise.</li> <li>Changed immediately if you suspect they are compromised.</li> </ul>	✓	✓	✓	✓
<b>VPN Gateways</b>	8.19 The Supplier shall ensure that VPN gateways are configured: <ul style="list-style-type: none"> <li>to offer and accept only the Recommended Profile and/or the Legacy Profile.</li> <li>to not allow negotiation of alternative cipher suites unless explicitly permitted by an administrator.</li> </ul>	✓	✓	✓	✓
	8.20 The Supplier shall adopt NCSC guidance when configuring VPN services.	✓	✓	✓	✓
<b>9 Operational Security</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Data Transfer</b>	9.1 The Supplier shall track authentication access data and on request shall give the Authority access to authentication logs relating to the service.	✓	✓	✓	✓
	9.2 The Supplier shall track security controls data and provide The Authority with access to security control logs relating to the service, this includes: <ul style="list-style-type: none"> <li>Anti-malware software,</li> <li>Firewalls</li> <li>Access controls list changes</li> <li>Services anything that perform a security function within the organisation.</li> </ul>	✓	✓	✓	
	9.3 The Supplier shall track DNS data and, on request, provide The Authority with access to DNS logs relating to the service.	✓	✓	✓	
	9.4 The Supplier shall track applications data relating to the service and provide, on request, the Authority with access.	✓	✓	✓	✓

	9.5 The Supplier shall track host applications and host operating system data and on request, provide the Authority with access.	✓	✓	✓	✓
	9.6 The Supplier shall track network devices and infrastructure data and upon request provide the Authority with access.	✓	✓	✓	
	9.7 The Supplier shall track cloud-based data including cloud management and compute services and provide on request the Authority with access.	✓	✓	✓	
<b>10 Cloud Security</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Cloud Register</b>	10.1 The Supplier shall have a detailed register of all cloud environments in use (provider, SLAs, contract length, services providers).	✓	✓	✓	✓
	10.2 The supplier shall regularly review the cloud register for accuracy and currency of cloud services in use.	✓	✓	✓	✓
<b>Cloud Incident Management</b>	10.3 The supplier shall have processes in place to establish incident notification mechanisms between the cloud providers and the Supplier's security operations center or equivalent team.	✓	✓	✓	✓
	10.4 The supplier shall ensure that cloud providers declare security incident information to the supplier, within a defined time period, with a detailed description to the effect on the supplier, which is required to be communicated with the Authority when relevant to the service provided.	✓	✓	✓	✓
	10.5 The supplier shall have SLAs in place with the cloud provider to ensure timely notification of incidents and their management.	✓	✓	✓	✓
<b>DDoS Protection</b>	10.6 The supplier shall ensure that their cloud environments automatically rate limit connections from clients upon detection upon a potential DDoS attack.	✓	✓	✓	✓
<b>Trusted Sources</b>	10.7 The Supplier shall ensure that cloud environments and their gateways only accept encrypted protocols from trusted and verified sources.	✓	✓	✓	✓
<b>Cloud Security Principles (NCSC)</b>	10.8 The Supplier is required to adhere to the following security protocols the NCSC "Cloud Security Principles", a copy of which can be found at: <a href="https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles">https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles</a> <ul style="list-style-type: none"> <li>"Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be</li> </ul>	✓	✓	✓	✓

	<p>adequately protected against tampering and eavesdropping;</p> <ul style="list-style-type: none"> <li>• "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;</li> <li>• "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;</li> <li>• "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;</li> <li>• "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;</li> <li>• "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Staff have access to Authority Data and/or The Authority System that those personnel be subject to appropriate security screening and regular security training;</li> <li>• "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;</li> <li>• "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other Suppliers;</li> <li>• "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for The Authority to securely manage The Authority use of the Service;</li> <li>• "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to</li> </ul>				
--	---	--	--	--	--

	<p>Service interfaces is constrained to authenticated and authorised individuals;</p> <ul style="list-style-type: none"> <li>• "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;</li> <li>• Security Principle 12: secure service administration" which, amongst other matters, requires that any IT system which is used for administration of a cloud service will have highly privileged access to that service;</li> <li>• "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide The Authority with the audit records it needs to monitor access to the Service and The Authority Data held by the Supplier and/or its Sub-contractors</li> <li>• "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Staff on the safe and secure use of the Information Management System.</li> </ul>				
<b>11 Physical and Environmental Security</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lite</b>
<b>Supplier Physical Entry controls</b>	11.6 The Supplier's staff shall adhere to Authority instructions at all times whilst on Authority premises.	✓	✓	✓	✓
	11.7 The Supplier shall ensure that all Supplier staff undertake Security Essentials Course delivered by the Authority within 3 months of commencement on the account. Failure to do so will lead to deactivation of their security pass.	✓	✓	✓	✓
	11.8 The Supplier shall ensure all personnel visiting the Authority's estate, restrict any official conversations on mobiles and landlines. All higher classification discussion must be conducted on appropriate systems.	✓	✓	✓	✓
<b>Secure Office Rooms/Facilities,</b>	11.9 The Supplier shall ensure that any home workers are vigilant to their surroundings and should consider the positioning of their equipment and assets.	✓	✓	✓	✓
<b>Procedures for Working in the Authority</b>	11.10 The Supplier shall ensure all personnel visiting the Authority's estate adhere to the Authority's working procedures, this includes: <ul style="list-style-type: none"> <li>• The clean desk policy which states all desks and spaces must be kept free of paper, notebooks, laptops etc.</li> </ul>	✓	✓	✓	✓

	<ul style="list-style-type: none"> <li>• All personnel must lock their laptop or computer whenever not in use.</li> <li>• In the UK, personal and work mobile phones must be stored in an acoustic box if the subject matter being discussed makes this necessary. At Post, phones are left in the designated rack if you're going into the secure area.</li> <li>• Visitors with security clearance are subject to the same rules on the Authority's UK estate as staff. Visitors without security clearance can carry their mobile devices on the Authority's UK estate with permission from the escorting officer; but if visitors are to be brought into areas where sensitive conversations are likely to be held or where there is classified communication equipment, they should be asked to leave their mobile devices at Reception. Secure lockers have been provided for this purpose.</li> <li>• There must be no inappropriate use of visitors' personal or work devices e.g. recording classified conversations, taking inappropriate photographs, voice or video recordings.</li> <li>• Lock the door when you go out of your office if there's no one else in the room.</li> <li>• If away from the desk for more than half an hour, visitors must lock away any OFFICIAL materials; other classified material should be placed in a secure container.</li> <li>• All protectively marked waste should be shredded or torn up and stored in classified waste bags. These should then be locked away at night and regularly collected for burning/pulping.</li> </ul>				
<b>Procedures for working Overseas at the Authority</b>	11.11 The Supplier shall ensure all personnel visiting the Authority's estate should read, sign and comply with the provided Post Security Regulations (PRS).	✓	✓	✓	✓
<b>Equipment and Equipment Maintenance</b>	11.12 The Supplier shall ensure equipment is routinely maintained to ensure it remains functional and to reduce the risk of failure.	✓	✓	✓	✓
	11.13 The Supplier shall maintain and update a maintenance schedule as evidence of servicing and repairs and on request provide to Authority as necessary.	✓	✓	✓	✓
	11.14 The Supplier shall ensure that the Authority's equipment is sited and protected from environmental threats, hazards, and unauthorised access.	✓	✓	✓	✓

	11.15 The Supplier shall ensure that all storage facilities are secured with keyed access by authorised key holders.	✓	✓	✓	✓
	11.16 The Supplier shall ensure that all information processing facilities handling sensitive data should be positioned and angled so that the risk of information being viewed by unauthorised personnel is reduced.	✓	✓	✓	✓
<b>Equipment Siting and Protection</b>	11.17 The Supplier shall ensure that information processing equipment is sited for easy access when required and securely stored when not in use.	✓	✓	✓	✓
<b>Supporting utilities</b>	11.18 The Supplier shall ensure that equipment is protected from disruptions caused by failure in supporting utilities.	✓	✓	✓	✓
<b>Cabling</b>	11.19 The Supplier shall ensure power and telecommunications cabling carrying data or supporting information services is protected from interception, interference or damage.	✓	✓	✓	✓
	11.20 The Supplier shall ensure cables are sited and protected adequately. Wherever possible, cables should be underground or otherwise protected and separated	✓	✓	✓	✓
<b>Removal of Assets from Premises</b>	<p>11.21 The Supplier shall ensure all personnel adhere to the Authority's procedures, when removing assets from the Authority's estates and traveling between Authority sites. The Supplier shall:</p> <ul style="list-style-type: none"> <li>request permission to remove assets from Authority estates. In the UK this will be from the Information Asset Owner (IAO) or Departmental Security Co-Ordinator (DSC); at Post, the IAO or Post Security Officer (PSO) will need to authorise</li> <li>leave in the office a list of the papers taken off site</li> <li>if travelling to a Post from the UK or from another mission, where possible, send papers securely ahead or send them electronically</li> <li>if using an officially provided mobile device in the UK, check with the Post Security Officer (PSO) whether this can be taken overseas. The PSO will inform whether local laws allow the use of encrypted devices.</li> <li>ensure officially provided mobile devices are not taken if going to (or transiting through) countries with high security threats. The PSO should be consulted to seek further guidance.</li> <li>ensure papers should be carried in a locked briefcase, preferably with a key or combination lock and kept with the person at all times.</li> <li>shutdown your laptop when leaving the house, Post, plane/ train, hotel or</li> </ul>	✓	✓	✓	✓

	<p>conference room as this ensures that all necessary safeguards are enabled.</p> <ul style="list-style-type: none"> <li>lock the screen whenever you're not using a device.</li> <li>be aware of people around as anyone can read over your shoulder when you are in a public space.</li> </ul>				
<b>Secure Disposal</b>	11.22 The Supplier shall check with the Authority and where permitted, that the Supplier ensures that end of life equipment is disposed of locally and that the data contained is erased safely. The Supplier shall consult the Authority IT help desk for safe disposal of end of life equipment.	✓	✓	✓	✓
	11.23 The Supplier shall check with the Authority to ensure that all items of equipment has been securely overwritten and removed of any sensitive data and licensed software prior to its disposal or reuse.	✓	✓	✓	✓
<b>Unattended User Equipment</b>	11.24 The Supplier shall ensure that any laptops or desktops are locked when unattended and switched off when not in use. Failure to do the stated will result in a security incident or breach.	✓	✓	✓	✓
<b>12. Sub- Contractors</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Sub- Contractors</b>	12.1 Where the Supplier enters into any subcontracting arrangement that requires the flow down of any obligation within this document, on request, the Supplier must be able to evidence that such obligations are being fulfilled.	✓	✓	✓	✓
<b>13. Vulnerability Management</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Information Management System</b>	13.1 The Supplier and Authority shall acknowledge that from time-to-time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Authority Data.	✓	✓	✓	✓
	13.2 The Supplier shall ensure that all identified vulnerabilities in the service being delivered must have an assigned severity rating and associated remediation plan. Such plan to be made available to the Authority on request.	✓	✓	✓	✓
<b>Patching</b>	13.3 The Supplier shall follow the requirements for patching laid out in the Vulnerability Management Standard for all systems and services utilised, developed or procured by the Authority. This applies to all	✓	✓	✓	✓



	<p>hardware, software, and cloud resource asset types including, but not limited to:</p> <ul style="list-style-type: none"> <li>• Internet facing websites and digital services.</li> <li>• End user client devices, such as laptops and mobile phones</li> <li>• Infrastructure devices, such as servers</li> <li>• Applications and sub-modules, such as anti-virus, mobile applications and web browser extensions</li> <li>• Internet-of-Things (IoT) devices</li> <li>• Network devices and sub-modules, such as routers and switches</li> </ul>				
	13.4 The Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within agreed upon deployment timescales as defined by the Vulnerability Management Standard.	✓	✓	✓	✓
	13.5 For any emergency patch, as defined by the Change Management Policy, the Supplier must adhere to the deployment of such patch within 3 days.	✓	✓	✓	
	<p>13.6 The Supplier shall conduct routine vulnerability scans, under a defined schedule agreed with the Authority. Vulnerability Scanning must:</p> <ul style="list-style-type: none"> <li>• include (Supplier/Authority) compliance requirements,</li> <li>• include Supplier risk assessment against (Supplier/the Authority) owned assets</li> <li>• include ad-hoc requirements such as a reactive scan to newly available threat intelligence</li> <li>• conducted following a significant change to any system</li> <li>• conducted on all related components following any incident perceived to have been a result of a vulnerability.</li> </ul>	✓	✓	✓	
<b>Security Management Plan</b>	13.7 Where required, the Supplier shall agree a Security Management Plan with the Authority based on the Authority's standard format.	✓	✓	✓	
<b>Tracking</b>	13.8 The Supplier shall track vulnerabilities throughout the vulnerability management lifecycle. Identified vulnerabilities that are assessed as Critical or High must be reported to the Authority upon discovery and no later than 24 hours after initial discovery. Furthermore any vulnerability assessed as having a significant impact to the running of the service or	✓	✓	✓	
<b>Security Monitoring</b>	13.9 The Supplier shall employ security monitoring to detect potential malicious behaviour and ensure authentication and authorisation events are logged and monitored for suspicious behaviour that may indicate a potential compromise.	✓	✓	✓	✓



	13.10 The Supplier shall control the flow of traffic through network boundaries and police content by proactively looking for attacks and evidence of compromised machines.	✓	✓	✓	
	13.11 The Supplier shall ensure Data Loss Prevention at egress points to inspect the contents of information and take appropriate action to prevent its inadvertent or malicious release.	✓	✓	✓	
<b>14. Communications Security</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Network Controls</b>	14.1 The Supplier shall ensure that network device and network hardening controls aligned to best practice are in place and actively monitored.	✓	✓	✓	✓
	14.2 To prevent data security breaches, the Supplier shall ensure that external connections to the network must: <ul style="list-style-type: none"> <li>• Be approved, documented (including purpose, approvals, and business justification)</li> <li>• be subject to periodic (at least 6 monthly) review, which should include checking for any unapproved external connections</li> <li>• be routed through a firewall</li> <li>• be designed and configured to ensure end to end protection of sensitive data in transit</li> <li>• restrict permitted traffic to only required ports, protocols, source, and destination addresses</li> <li>• apply the 'default deny' principle (i.e. any traffic that is not explicitly allowed must be blocked);</li> <li>• not create a bridge between networks of different trust (i.e. production &amp; corporate, public &amp; private, etc.).</li> </ul>	✓	✓	✓	✓
	14.3 The Supplier shall have Distributed Denial of Service (DDoS) protection in place for any internet facing services to detect and prevent such an attack. This can include, but is not limited to, rate limiting and packet dropping.	✓	✓	✓	✓
	14.4 The Supplier shall ensure Intrusion Detection Technology is deployed at all ingress points of the network, complete with alerting systems and clear processes on how detected intrusions will be managed in order to block any malicious intrusions to the network.	✓	✓	✓	✓
	14.5 The Supplier shall ensure Firewalls are in place at all points where	✓	✓	✓	

	data and traffic enters and exits the network, and rulesets are regularly reviewed, including, as required by the Authority (at a minimum every six months).				
	14.6 The Supplier must ensure DNS requests from unknown networks are blocked to prevent requests to external malicious websites.	✓	✓	✓	✓
<b>Security of Network Services</b>	14.7 If appropriate to the services provided, the Supplier shall adhere to the network services agreement outlined by the Authority. If the Supplier is using its own network, the Supplier must include all the relevant security measures taking into consideration the Authority's security requirements.	✓	✓	✓	
	14.8 The Supplier shall maintain an up-to-date and approved network diagram which includes all aspects of the network relevant to the Authority's services, including firewalls, routers, cloud servers, VPN connections and data center MLPS connections.	✓	✓	✓	
<b>Segregation in Networks</b>	14.9 The Supplier shall ensure that any enterprise wireless networks have segregated corporate and guest instances. The guest wireless network should only allow direct connection to the internet and should be ring fenced from any corporate resources.	✓	✓	✓	
	14.10 The Supplier shall ensure their corporate wireless network is secured through encryption protocols such as WPA2/3 and security features such as SSID hiding and MAC/IP filtering.	✓	✓	✓	✓
	14.11 The Supplier shall ensure that Connection to the corporate wireless network is subject to adequate authentication measures, such as Multi Factor Authentication (MFA).	✓	✓	✓	✓
<b>Information Transfers Policy and Procedures</b>	14.12 The Supplier shall ensure that there are formal information transfer policies and procedures in place to protect the transfer of information through the use of all types of communication facilities. This must cover the security risks in relation to the confidentiality, integrity and availability of the Authority's data being transferred.	✓	✓	✓	✓
	14.13 The Supplier shall have Network flow diagrams in place, which clearly outline any flows involving the Authority's data.	✓	✓	✓	✓
	14.14 The Supplier shall record and maintain the scope and configuration of the service being supplied which should be available upon request.	✓	✓	✓	✓
	14.15 The Supplier shall ensure that any suspicious activity on any network is logged, monitored, and investigated	✓	✓	✓	✓

	in line with their standard incident management procedures. These include incidents such as detection of anomalous user behaviour, attempted DDoS attacks, and others.				
	14.16 The Supplier shall ensure a network data loss prevention (DLP) solution is implemented on the network which processes the Authority's data, which is configured to log, monitor, alert and take action upon unusual activity in user channels. This DLP solution must establish clear policies on where data can be sent, and who has access to data transfer channels.	✓	✓	✓	✓
	14.17 The Supplier shall ensure that Software, services or features that send information outside of the network boundary are disabled unless approved and appropriately configured for use by the Authority.	✓	✓	✓	✓
	14.18 The Supplier shall define and implement a policy to control the exchanging of information via removable media which is available on request by Authority.	✓	✓	✓	
<b>Electronic Messaging</b>	14.19 The Supplier shall ensure that browser-based protection is in place and blocks at a minimum the data transfer functionality of browser-based mail (e.g. Gmail, Hotmail), file sharing sites (e.g. Dropbox, Google Drive), and social media sites (e.g. Facebook, Twitter).	✓	✓	✓	
	14.20 The Supplier shall ensure email content filtering tools are in place to ensure the sending of non-public Authority data (e.g. sending of card data, account information and personal data etc.) is flagged, reviewed and blocked where appropriate.	✓	✓	✓	
	14.21 If relevant, the Supplier shall ensure that they employ a cloud access security broker (CASB) or equivalent shadow cloud management service is in place to help detect and apply controls to shadow cloud usage.	✓			
<b>Confidentiality or Non-Disclosure Agreements</b>	14.22 The Supplier shall comply with the confidentiality and non-disclosure agreements outlined as part of the service agreement.	✓	✓	✓	✓
<b>15. Systems Acquisition, Development and Maintenance</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Securing Application</b>	15.1 The Supplier shall ensure that a web application firewall is in place to block any unauthorised traffic to each	✓	✓	✓	

<b>Services on Public Networks</b>	application interface within and across said application.				
	15.2 The Supplier shall ensure that application interface inputs have been modelled against expected activity for a user of a specific level, to ensure anomalous traffic is rejected and alerted on.	✓	✓	✓	
	15.3 The Supplier shall implement controls to monitor application interface traffic, both inputs and outputs, and block and alert on any anomalous/suspicious activity where necessary.	✓	✓	✓	
<b>Secure Development Environment</b>	15.4 The Supplier shall ensure that there is a dedicated development environment in place in which coding and other development practices are performed separately from production environments.	✓	✓	✓	
	15.5 The Supplier shall not routinely use live data in the production environments. The Supplier must have explicit written approval from the Authority for the use of live data which must be logged and monitored at a minimum. Data must be anonymised as far as possible, carefully selected and secured for the period of testing. Data must be securely deleted upon testing completion.	✓	✓	✓	✓
	15.6 The Supplier shall perform security tests on applications whilst in development to ensure they are secure prior to release and include consideration of recent threat intelligence.	✓	✓	✓	✓
	15.7 The Supplier shall test all aspects of the application, including dependent libraries as part of the security testing.	✓	✓	✓	✓
	15.8 The Supplier shall identify vulnerabilities and ensure they are remediated appropriately (tracked through to completion/risk accepted).	✓	✓	✓	✓
<b>Systems Change Control Procedures</b>	15.9 The Supplier shall ensure that changes to systems within the development lifecycle must be controlled by the use of formal change control procedures, which must be aligned with and support operational control procedures.	✓	✓	✓	✓
	15.10 The Supplier shall ensure that all code repositories have an in-built version control capability. A source code management solution must be	✓	✓	✓	✓

	used to protect version application materials.				
	15.11 The Supplier shall ensure that application code, binaries and any associated libraries are obtained and or utilised from a reputable source, reviewed for integrity, and approved before using.	✓	✓	✓	✓
<b>Technical Review of Applications after OS Changes</b>	15.12 The Supplier shall ensure that when operating platforms are changed, business critical applications are reviewed and tested to ensure there is no material impact on the Authority's operations or security.	✓	✓	✓	
	15.13 The Supplier shall test operating system changes in a development or test environment where critical business applications can be checked for compatibility with the changed OS to ensure compatibility and continuity of service provision.	✓	✓	✓	
	15.14 The Supplier shall follow the Authority's standard change management controls when going through the testing of operating system changes.	✓	✓	✓	
<b>Restrictions on Changes to Software Packages</b>	15.15 The Supplier shall limit modifications of software packages to necessary changes. All changes must go through the Authority's change control procedure.	✓	✓	✓	
<b>Secure System Engineering Principles</b>	15.16 The Supplier shall establish and adhere to principles for engineering secure systems to any information system implementation efforts.	✓	✓	✓	✓
	15.17 The Supplier shall consider, assess, formally document and mandate the selection and application of such principles whenever development is being carried out.	✓	✓	✓	✓
	15.18 The Supplier shall align secure system engineering principles against risk levels.	✓	✓	✓	
<b>System Security Testing</b>	15.19 Through delivery of the service the Supplier shall be required to test the security functionality during development. Testing of security functionality must be approved by the Authority in writing.	✓	✓	✓	
	15.20 The Supplier shall document security testing expected outcomes before testing commences and should be based on business requirements for security.	✓	✓	✓	✓
<b>16. Information Security Incident Management</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>

<b>Responsibilities and Procedures</b>	16.1 The Supplier shall provide a suitably qualified and experienced person (SQEP) as a point of contact for IT systems and services, for the purpose of escalation for Incident Management.	✓	✓	✓	✓
<b>Response to Security Incidents</b>	16.2 The Supplier shall provide Incident Management Responses and notification time frames when responding to a security breach involving the Authority.	✓	✓	✓	✓
	16.3 The Supplier shall work collaboratively with the Authority to support investigations into the root cause of a security breach.	✓	✓	✓	✓
	16.4 The Supplier shall have a documented policy and or procedure that establishes management responsibilities and procedures for a quick, effective and orderly response to incidents including: <ul style="list-style-type: none"> <li>• Availability of offline copies of Incident Management playbooks/procedures</li> <li>• Categorisation, e.g. type and potential impact, and how to manage them</li> <li>• Triage and corrective actions to support SLAs</li> <li>• Root cause and trend analysis</li> <li>• Escalation internally and when the Authority would be notified</li> <li>• Engagement of specialist companies, e.g. who, for what type of incident and how to contact them</li> <li>• Reasonable access to necessary information to assist in any investigation</li> <li>• Process if criminal or wrongdoing are suspected</li> <li>• Containment, preservation of evidence</li> <li>• Out-of-band communication tooling segregated from enterprise network</li> </ul>	✓	✓	✓	
	16.5 The Supplier shall proactively verify that security controls are providing the intended level of security confirmation of this being made available upon request by the Authority.	✓	✓	✓	
<b>17. Information Security Aspects of Business Continuity Management</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Planning Information Security Continuity</b>	17.1 The Supplier shall include requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster as part of their Business Continuity Policy, and Business Continuity Plan.	✓	✓	✓	✓

	17.2 The Supplier shall define outline key events and scenarios which might impact information security to demonstrate that the Supplier understands and can address risks to information security continuity, take steps to reduce the likelihood of interruptions, mitigate the impact from incidents and manage the recovery of services in line with agreed recovery timescales.	✓	✓	✓	✓
	17.3 The Supplier shall incorporate controls, as part of their business continuity plan, which ensure information processing facilities are implemented with redundancy sufficiency to meet availability requirements.	✓	✓	✓	✓
	17.4 The Supplier shall maintain the policy and business continuity documentation and controls to ensure they remain relevant and continue to meet the principle aim of ensuring the continued seamless provision of services, with a copy of the documents being provided to the Authority on request.	✓	✓	✓	✓
<b>Implementing Information Security Continuity</b>	17.5 The Supplier shall define responsibilities, activities, owners, timescales, mitigating work to be undertaken (beyond risks and policies already in operation e.g. crisis communications) and ensure these are provided to the Authority on request.	✓	✓	✓	✓
	17.6 The Supplier shall outline a management structure and relevant escalation trigger points to ensure that if and when an event increases in severity the relevant escalation to the Authority is made effectively and in a timely manner. It should also be made clear when there is a return to business as usual and any BCP processes stop confirmation is provided to the Authority in writing.	✓	✓	✓	✓
<b>Verify Review and Evaluate Information Security Continuity</b>	17.7 The Supplier shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during these situations.	✓	✓	✓	✓
	17.8 The Supplier shall ensure they test redundant components and systems periodically to ensure that fail-over will be achieved in a reasonable time-frame. Redundant components must be protected at the same level or greater than the primary components.	✓	✓	✓	✓
	17.9 The Supplier shall provide annual evidence to the Authority that these controls have been tested, reviewed and evaluated periodically to ensure they are maintained against changes in the business, technologies and risk levels.	✓	✓	✓	

<b>18. Compliance and Assurance</b>		<b>Extended</b>	<b>Developer</b>	<b>Consultancy/ Professional Services</b>	<b>Lit e</b>
<b>Independent Reviews of Information Security</b>	18.1 The Supplier shall demonstrate routine reviews of information security.	✓	✓	✓	✓
<b>Cyber Essentials+</b>	18.2 Supplier shall annually renew Cyber Essentials Scheme Plus Certification or equivalent standards that are approved by the Authority.	✓	✓	✓	✓



Document Definitions	
<b>"Access Control lists"</b>	Shall refer to a user access lists for all relevant applications and networks, detailing the up-to-date and accurate access rights of relevant users from a reliable source.
<b>"Authority Data"</b>	Shall refer to the data held by the Authority.
<b>"Authority's Security Requirements"</b>	Shall refer to the requirements outlined in this document.
<b>"Cloud"</b>	Shall refer to an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data
<b>"Code of Connection"</b>	Shall mean a level of assurance that your systems, which access and use Authority information and systems, are managed and controlled to acceptable levels.
<b>"Contract Period"</b>	Shall refer to any number of days, as outlined in the contract, that the contract will run for.
<b>"Contractor's Systems Environment"</b>	Shall refer to any IT systems provided by the Contractor (and any Sub-Contractor) which are to be used for the provision of services.
<b>"Contractor"</b>	Shall refer to an organisation or individual who is outsourced by the Authority to undertake work for the Authority.
<b>"Cyber Essentials Plus"</b>	Shall refer to the Government-backed, industry supported scheme managed by the NCSC with higher level of security requirements to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC. Cyber Essentials Plus still has the Cyber Essentials trademark simplicity of approach, and the protections you need to put in place are the same, but for Cyber Essentials Plus a hands-on technical verification is performed.
<b>"Cyber Essentials"</b>	Shall refer to the Government-backed, industry supported scheme managed by the NCSC with higher level of security requirements to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.
<b>"Data Protection Officer (DPO)"</b>	Shall mean a role which ensures their organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.
<b>"Entitlement Level"</b>	Shall mean assignments to any given role, and roles are assigned to users, based on least privileged access.
<b>"Forensically Unrecoverable"</b>	Shall refer to data or information that has no recovery possible.
<b>"Group Domain of Interpretation (GDOI)"</b>	Shall refer to a cryptographic protocol for group key management.
<b>"HMG Baseline Personnel Security Standard"</b>	Shall refer to the pre- employment controls for all civil servants, members of the Armed Forces, temporary staff, and government contractors generally. It's rigorous and consistent application also underpins national security vetting.

## OFFICIAL

<b>“Information Security Management System (ISMS)”</b>	Shall refer to the set of policies, processes and systems designed, implemented, and maintained by the Contractor to manage Information Security Risk as certified by ISO/IEC 27001.
<b>“Information Security Manager”</b>	Shall refer to the person appointed by the Contractor with the appropriate experience, Authority, and expertise to ensure that the Contractor complies with the Authority’s Security Requirements.
<b>“Information Security Risk”</b>	Shall refer to any risk that might adversely impact the engagement.
<b>“Information Security”</b>	Shall refer to a) the protection and preservation of: i) the Confidentiality, Integrity and Availability of any Authority Assets, the Authority’s Systems Environment (or any part thereof) and the Contractor’s Systems Environment (or any part thereof); ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and b) compliance with all Law applicable to the processing, transmission, storage and disposal of Authority Assets.
<b>“Office of the Data Protection Officer (ODPO)”</b>	Shall refer to a mandatory role appointed by HMRC to meet the requirements of the data protection legislation.
<b>“Parties”</b>	Shall refer to any public or private commercial entity, (B) any officer, director, employee, agent or representative of any public or private commercial entity, or (C) any relative or family or household member of any of the persons listed in clauses (A) or (B) of this definition.
<b>“Penetration Tests”</b>	Shall refer to a simulated attack on any Authority Assets, the Authority’s Systems Environment (or any part thereof) or the Contractor’s Systems Environment (or any part thereof).
<b>“Risk Assessment”</b>	Shall refer to risk assessment is a framework that helps organisations identify, evaluate, and treat risks that could affect their information security processes.
<b>“Risk Management Policy”</b>	Shall refer to the policy which outlines the approach to identifying, analysing, evaluating and treating risks at all levels of the organisation.
<b>“Risk Profile”</b>	Shall refer to the description of any set of risks. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.
<b>“Risk Profile”</b>	Shall refer to a description of any set of risks. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.
<b>“Role Based Access Control Model”</b>	Shall refer to restricting system access to authorised users, and to implementing mandatory access control or discretionary access controls.
<b>“Security Risk Management Policy”</b>	Shall refer to the policy which defines the process of identifying, evaluating, and treating risks around the organisation’s information and cyber security. It addresses uncertainties around those assets to ensure the desired business outcomes are achieved.
<b>“Security Test”</b>	Shall include, but not be limited to, penetration test, vulnerability scan, availability test and any other security related test and audit.
<b>“Services”</b>	Shall refer to the provision of a specialised activity, function or product.
<b>“SQEP”</b>	Shall refer to a suitably qualified and experience person(s).

## OFFICIAL


---

<b>“Sub-Contractor”</b>	Shall refer to an organisation or individual who is outsourced by a contractor to undertake work for the Authority.
<b>“Supplier</b>	Shall refer to an organisation or individual who is contracted to provide a service or product to the Authority.
<b>“The Authority”</b>	Shall refer to the Authority.
<b>“Vulnerability Scan”</b>	Shall mean an ongoing activity to identify any potential vulnerability in any Authority Assets, the Authority’s Systems Environment (or any part thereof) or the Contractor’s Systems Environment (or any part thereof).

## OFFICIAL

## Section 4 - Schedule of Prices &amp; Rates

## Instructions

		
Foreign, Commonwealth & Development Office		
INSTRUCTIONS - HARDSHIP AND COST OF LIVING DATA PROCESSING & PROVISION		
<b>To note</b> Cf. ATTACHMENT XX - 9629 - INSTRUCTIONS TO TENDER, ATTACHMENT XX - 9629 - STATEMENT OF SERVICE REQUIREMENTS, and ATTACHMENT XX - 9629 - CONTRACT TERMS and CONDITIONS. <b>Tab 1. Cost Summary:</b> For the deliverables 'Provision of Hardship data (annual requirement)', 'Provision of Cost of Living Allowance (COLA) data - March worldwide costing exercise', and 'Provision of Cost of Living Allowance (COLA) data - September update', the Authority has used the cost assumption that 282 data sets will be required in each case. For the deliverables 'Provision of Cost of Living Allowance (COLA) data - June interim review' and 'Provision of Cost of Living Allowance (COLA) data - December interim review', the Authority has estimated that 25 data sets will be required in each case, based on the previous year. However, <u>the Authority does not guarantee this volume of activity as requirements can vary year-on-year. Total cost for Years 6 and 7 will be subject to C4. PRICE ADJUSTMENT in ATTACHMENT XX - 9629 - CONTRACT TERMS AND CONDITIONS</u> (fixed prices will remain unchanged for a period of five years, thereafter indexation may be applied, as agreed by both parties). <u>The Authority's commercial evaluation will be based on 'Total cost over seven years - based on pricing scenario', to enable like-for-like pricing consideration.</u> <b>Tab 2. Schedule of Prices and Rates:</b> <u>The fixed prices stated therein constitute the only amounts payable by the Authority to the Potential Provider for providing the services.</u> The fixed prices shall include <u>all costs and expenses incurred either directly or indirectly by the Potential Provider in providing the services</u> , including (but not limited to) staffing, mobilisation, transition, and provision of Management and Key Performance Indicator Review reporting and attendance at meetings and presentations as required by the Authority. Therefore, these <u>rates should be sustainable for suppliers throughout the life of the contract.</u> The Potential Provider undertakes to make all reasonable efforts to ensure that all services are delivered at the best possible market price, in line with the Authority's requirements to ensure Value for Money. For the purpose of this contract, Value for Money is defined as the optimum combination of whole life costs and quality to meet the Authority's requirements. <u>The Authority reserves the right to seek clarifications on any element of pricing submitted by bidders.</u> All prices must be stated in £ Sterling and inclusive of VAT. <b>Tab 3. Staffing:</b> Staffing information has been requested for information and transparency purposes only. <b>Tab 4. Commentary:</b> Commentary has been requested for information and transparency purposes only. <u>This does not form part of our tender evaluation method. The Potential Provider must not use the free text box to present qualifications to the contents of the Invitation to Tender (ITT), nor any bidder response to the Technical Evaluation Questions.</u> Qualifications presented may lead to a Potential Provider being disqualified at the absolute discretion of the Authority. This free text box is the prime means of recording and evaluating supplier's costs, including (but not limited to) margins, incidentals and profit. The Potential Provider should include any pricing assumptions around any aspect of the submitted fixed prices and any rationale behind stated profit margins i.e. % management fee by deliverable (or lack thereof, if applicable) so that we can understand the Potential Provider's commercial expectations and have a clearer picture of the sustainability of our requirement. We suggest responses are limited to 750 words. <b>Tab 5. Payment Plan:</b> Payment plan information has been requested for planning and administration purposes only.		
<b>Tab</b>	<b>Purpose</b>	<b>Action required by the Potential Provider</b>
<b>1. Cost Summary</b>	For evaluation and population of payment amounts in tab	Complete yellow cell with supplier name. Check the blue cells to show Year 1-7 costs by Deliverable and total costs have auto-completed correctly with the fixed prices from tab 2. Schedule of Prices and Rates, multiplied by 282 for the Deliverables: 'Provision of Hardship data (annual requirement)', 'Provision of Cost of Living Allowance (COLA) data - March worldwide costing exercise', and 'Provision of Cost of Living Allowance (COLA) data - September update'; or by 25 for the deliverables 'Provision of Cost of Living Allowance (COLA) data - June interim review' and 'Provision of Cost of Living Allowance (COLA) data - December interim review'.
<b>2. Schedule of Prices and Rates</b>	For population of tab 1. Cost Summary.	Complete the yellow cells with fixed prices.
<b>3. Staffing</b>	For information and transparency purposes only.	Complete the yellow cells as indicated. Check the orange cells to show net costs of positions and totals have auto-completed
<b>4. Commentary</b>	For information and transparency purposes only.	Complete the yellow cells with the % (between 10 and 20) of Total Fixed Prices (£) to be put at risk/deducted in line with Key Performance Indicators 1-3 in the <b>STATEMENT OF SERVICE REQUIREMENTS</b> attachment. Complete the free text box with any pricing assumptions around any aspect of the submitted fixed prices and any rationale behind stated profit margins i.e. % management fee by deliverable (or lack thereof, if applicable).
<b>5. Payment Plan</b>	For planning and administration purposes only.	Complete the yellow cells with invoice dates. Check the orange cells to show the resultant payment date (within 30 days of receipt of a valid invoice) have auto-completed correctly. Check the blue cells to show the payment amounts have auto-completed correctly with the Deliverable costs from tab 1. Cost Summary (not including 'Provision of Interim Post data/50 data sets' as this is an ad hoc

1. Cost summary  
[REDACTED]

2. Schedule of Prices and Rates  
[REDACTED]

3. Staffing – for info. – NOT USED

4. Commentary – for info.

[REDACTED]

5. Payment Plan – for planning

[REDACTED]



Section 5 - NOT USED

Section 6 - Successful Tenderers Response to ITT  
[REDACTED]