HM Revenue & Customs

100 Parliament Street

Westminster

London SW1A 2BQ

and

Netcompany UK Limited.

1st Floor, Northburgh House

10 Northburgh Street

London, EC1V 0AT

United Kingdom

AGREEMENT relating to National Transit Computer System (NTCS) – Trader Testing

Commercial Directorate Ref: SR1253962880

Form of Agreement

This Agreement is made between the Commissioners for Her Majesty's Revenue and Customs (the "**Authority"**) of 100 Parliament Street, Westminster, London, SW1A 2BQ and Netcompany UK Limited (the "**Supplier"**)] whose company number is 08568559 and whose main or registered office is at 1st Floor, Northburgh House, 10 Northburgh Street, London, EC1V 0AT, United Kingdom.

This Agreement is effective from and including 21st December 2022 ("**Effective Date**") and shall expire on 20th December 2023 ("**Expiry Date**").

It is agreed that:

This Form of Agreement together with the Terms and Conditions and Schedules are the documents that form the Agreement.

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

Signed for and on behalf of:

	The Commissioners for HM Revenue & Customs:		**Netcompany UK Limited**
Signature:		Signature:	
Name:	[redacted]	Name:	[redacted]
Capacity:	IT Assistant Commercial Director	Capacity:	Country Managing Partner
Date:		Date:	
Address:	[redacted]	Address:	[redacted]

Telephone:	[redacted]	Telephone:	[redacted]
email:	[redacted]	email:	[redacted]

TERMS AND CONDITIONS

Definitions

1.1 In this Agreement, unless otherwise provided or the context otherwise requires the following expressions shall have the meanings set out below:

"Agreement"	the contract between (i) the Authority acting as part of the Crown and (ii) the Supplier;
"Authority"	has the meaning given in the Form of Agreement;
"Authority Data"	(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 Supplier by or on behalf of the Authority; and/or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or (b) any Personal Data for which the Authority is the Controller, or any data derived from such Personal Data which has had any designatory data identifiers removed so that an individual cannot be identified.
"BPSS"	the HMG Baseline Personnel Security Standard staff vetting procedures, issued by the Cabinet Office Security Policy Division and Corporate Development Group;
"Central Government Body"	a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: (a) Government Department; (b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal); (c) Non-Ministerial Department; or (d) Executive Agency;
"Charges"	the charges for the Services as specified in Paragraph A5 of Schedule 1.2 (Pricing);
"Confidential Information"	all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
"Default"	any breach of the obligations of the relevant Party (including

	abandonment of this Agreement in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement: (a) in the case of the Authority, of its employees, servants, agents; or (b) in the case of the Supplier, of its sub-contractors or any Supplier Personnel, in connection with or in relation to the subject-matter of this Agreement and in respect of which such Party is liable to the other;
	a.
"Effective Date"	has the meaning given in the Form of Agreement;
"Expiry Date"	has the meaning given in the Form of Agreement;
"FOIA"	the Freedom of Information Act 2000;
"GDPR"	the General Data Protection Regulation (Regulation (EU) 2016/679);
"Information"	has the meaning given under section 84 of the FOIA;
"Intellectual Property Rights"	patents, inventions, trademarks, service marks, logos, design rights (whether registerable or otherwise), applications for any of the foregoing, copyright, database rights, domain names, trade or business names, moral rights and other similar rights or obligations whether registrable or not in any country (including but not limited to the United Kingdom) and the right to sue for passing off;
"Law"	any applicable Act of Parliament, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of section 2 of the European Communities Act 1972, regulatory policy, guidance or industry code, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
"Losses"	losses, liabilities, damages, costs and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise;
"Key Personnel"	any Supplier Personnel specified as such in Paragraph 4 (Contract Management Roles and Dispute Escalation Points) of Schedule 3 (Contract Management Plan and Management Information) or otherwise notified as such by the Authority to the Supplier in writing;
"Occasion of Tax Non-Compliance"	(a) any Tax return of the Supplier and/or its subcontractor and/or any non-submission of a Tax return (whether deliberate or by omission) by the Supplier and/or its subcontractor to the Relevant Tax Authority on or after 1 October 2012 is found to be incorrect as a result of:

(iii) a Relevant Tax Authority successfully challenging the Supplier or relevant sub-contractor under the General Anti Abuse Rule or the Halifax Abuse Principle or TAAR or under any Tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti Abuse Rule or the Halifax Abuse Principle or TAAR;

(iv) the failure of an avoidance scheme which the Supplier or relevant sub-contractor was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or

(b) the Tax affairs of the Supplier or any of its sub-contractors have given rise to a criminal conviction in any jurisdiction for Tax related offences within the last five (5) years which is not spent at the Effective Date or to a civil penalty for fraud or evasion within the last three (3) years;

(c) For these purposes :

(i) a return is "submitted" when it is first submitted to the Relevant Tax Authority and any subsequent amendments or re-submissions are to be ignored; and

(ii) a Relevant Tax Authority will not be deemed to have "successfully challenged" the Supplier or a sub-contractor until an appeal against such challenge is no longer possible.

"Party"	the Supplier or the Authority (as appropriate) and "Parties" shall mean both of them;
"Personal Data"	has the meaning given in the GDPR;
"Purchase Order Number"	the Authority's unique number relating to the supply of the Services;
"Request for Information"	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term "request" shall apply);
"**Reimbursable Expenses**"	reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Authority's expenses policy Schedule 1.1 Annex 1 HMRC TRAVEL & SUBSISTENCE POLICY current from time to time, but not including: (a) travel expenses incurred as a result of Supplier Personnel travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Authority otherwise agrees in advance in writing; and

(b) subsistence expenses incurred by Supplier Personnel whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed;

"Relevant Tax Authority"	HMRC, or, if applicable, a tax authority in the jurisdiction in which the Supplier is established, resident or liable to any Tax;
"Services"	the services to be supplied by the Supplier to the Authority under the Agreement, including the provision of any Goods;
"Services Start Date"	the services start date set out in Paragraph A4 of Schedule 1.1 (Services Description);
"Specification"	the specification for the Services (including as to quantity, description and quality) as specified in Paragraph A6 of Schedule 1.1 (Services Description);
"Supplier Personnel"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any sub-contractor of the Supplier engaged in the performance of the Supplier's obligations under the Agreement;
"Supplier"	has the meaning given in the Form of Agreement;
"Tax"	means: (a) all forms of tax whether direct or indirect; (b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction; (c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions. levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and (d) any penalty, fine, surcharge, interest, charges or costs relating to any of the above, in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;
"Term"	the period from the Effective Date to the Expiry Date as such period may be extended in accordance with Clause 5.2 or terminated in accordance with the terms and conditions of the Agreement;
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
"Working Day"	a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

1.2 In these terms and conditions, unless the context otherwise requires:

1.2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;

1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;

1.2.3 the headings to the clauses of these terms and conditions are for information only

and do not affect the interpretation of the Agreement;

1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and

1.2.5 the word 'including' shall be understood as meaning 'including without limitation'.

1.3 In the event of any conflict between the terms of Schedule 1.1 (Services Description) and any other term of this Agreement, the terms of Schedule 1.1 shall prevail.

2 Supply of Services

2.1 In consideration of the Authority's agreement to pay the Charges, the Supplier shall supply the Services to the Authority from the Services Start Date until the end of the Term subject to and in accordance with the terms and conditions of the Agreement.

2.2 In supplying the Services, the Supplier shall:

2.2.1 co-operate with the Authority in all matters relating to the Services and comply with all the Authority's written instructions;

2.2.2 perform the Services with all reasonable care, skill and diligence in accordance with good industry practice in the Supplier's industry, profession or trade;

2.2.3 use Supplier Personnel who are suitably skilled and experienced to perform tasks assigned to them, and in sufficient number to ensure that the Supplier's obligations are fulfilled in accordance with the Agreement;

2.2.4 ensure that the Services shall conform with all descriptions and specifications set out in the Specification;

2.2.5 comply with all applicable Laws; and

2.2.6 provide all equipment, tools and vehicles and other items as are required to provide the Services.

2.3 If the Authority informs the Supplier in writing that the Authority reasonably believes that any part of the Services does not meet the requirements of the Agreement or differs in any way from those requirements, and this is other than as a result of a Default by the Authority, the Supplier shall at its own expense re-schedule and carry out the Services in accordance with the requirements of the Agreement within such reasonable time as may be specified by the Authority and agreed by the Supplier acting reasonably.

3 Supply of Goods

3.1 Where, as part of the Services, the Supplier is to sell goods or equipment ("**Goods**") to the Authority:

3.1.1 the relevant Goods and their prices shall be as set out in Schedule 1.1 (Services Description);

3.1.2 the Supplier shall supply and, where relevant, install the Goods in accordance with the relevant specification;

3.1.3 the Supplier shall ensure that the Goods are free from material defects in design, materials and workmanship and remain so for twelve (12) months after delivery;

3.1.4 if following inspection or testing the Goods do not conform with the relevant specification, the Authority shall inform the Supplier and the Supplier shall

immediately take such remedial action as is necessary to ensure compliance; and

3.1.5 Without prejudice to any other rights or remedies of the Authority a) the title in the Goods shall pass to the Authority at the time of payment of the respective Goods price to the Supplier. and b) the risk in the Goods shall pass to the Authority at the time of Payment or such earlier time as required at the Authority's sole discretion.

4 Warranties

4.1 The Supplier represents and warrants that:

4.1.1 in the three years prior to the Effective Date, it has been in full compliance with all applicable securities and Tax Laws and regulations in the United Kingdom and in the jurisdiction in which it is established;

4.1.2 it has notified the Authority in writing of any Occasions of Tax Non-Compliance and any litigation, enquiry or investigation in which it or its Subcontractors is/are (as appropriate) involved that is in connection with, or which may lead to any Occasion of Tax Non-Compliance;

4.1.3 no profit warnings, 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 Supplier 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 Supplier's assets or revenue; and

4.2 If at any time a Party becomes aware that a representation or warranty given by it under Clause 4.1.1 or 4.1.2 has been breached, is untrue, or is misleading, it shall immediately notify the other Party of the relevant occurrence in sufficient detail to enable the other Party to make an accurate assessment of the situation.

5 Term

5.1 The Agreement shall take effect on the Effective Date and shall expire on the Expiry Date, unless it is otherwise extended in accordance with Clause 5.2 or terminated in accordance with the terms and conditions of the Agreement.

5.2 The Authority may extend the Agreement for a period of up to 2 x 12 months by giving not less than 10 Working Days' notice in writing to the Supplier prior to the Expiry Date. The terms and conditions of the Agreement shall apply throughout any such extended period.

6 Charges, Payment and Recovery of Sums Due

6.1 The Charges for the Services shall be as set out in Schedule 1.1 (Services Description) and shall be the full and exclusive remuneration of the Supplier in respect of the supply of the Services. Unless otherwise agreed in writing by the Authority, the Charges shall include every cost and expense of the Supplier directly or indirectly incurred in connection with the performance of the Services.

6.2 The Supplier shall invoice the Authority as specified in the Agreement. Each invoice shall include such supporting information required by the Authority to verify the accuracy of the invoice ("**Supporting Documentation**"), including the relevant Purchase Order Number (and CD Reference) and a breakdown of the Services supplied in the invoice period.

6.3 To facilitate payment, the Supplier shall use an electronic transaction system chosen by the Authority and shall:

6.3.1 register for the electronic transaction system in accordance with the instructions of the Authority;

6.3.2 allow the electronic transmission of purchase orders and submitting of electronic invoices via the electronic transaction system;

6.3.3 designate a Supplier representative as the first point of contact with the Authority for system issues; and

6.3.4 provide such data to the Authority as the Authority reasonably deems necessary for the operation of the system including, but not limited to, electronic catalogue information.

6.4 The Authority has implemented its electronic transaction system (myBUY). Each invoice and any Supporting Documentation required to be submitted in accordance with this Clause 6 shall be submitted by the Supplier, as directed by the Authority from time to time via myBUY

6.5 The Supplier acknowledges and agrees that should it commence Services without a Purchase Order Number:

6.5.1 the Supplier does so at its own risk; and

6.5.2 the Authority shall not be obliged to pay the Charges without a valid Purchase Order Number having been provided to the Supplier.

6.6 The Authority shall regard an invoice as valid only if it complies with the provisions of this Clause 6. The Authority shall promptly return any non-compliant invoice to the Supplier and the Supplier shall promptly issue a replacement, compliant invoice.

6.7 In consideration of the supply of the Services by the Supplier, the Authority shall pay the Supplier the invoiced amounts no later than 30 days after receipt of a valid invoice which includes a valid Purchase Order Number.

6.8 If there is a dispute between the Parties as to the amount invoiced, the Authority shall pay the undisputed amount. The Supplier shall not suspend the supply of the Services unless the Supplier is entitled to terminate the Agreement for a failure to pay undisputed sums in accordance with Clause 20.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in Clause 23.

6.9 If a payment of an undisputed amount is not made by the Authority by the due date, then the Authority shall pay the Supplier interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.

6.10 If any sum of money is recoverable from or payable by the Supplier under the Agreement (including penalties but excluding any damages which the Supplier is liable to pay to the Authority in respect of any breach of the Agreement), that sum may be deducted following agreement between Parties from any sum then due, or which may come due, to the Supplier under the Agreement. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Authority in order to justify withholding payment of any such amount in whole or in part.

Expenses

6.11 Where the Authority expressly agrees in writing, the Supplier shall be entitled to be reimbursed by the Authority for Reimbursable Expenses (in addition to being paid the relevant Charges), provided that such Reimbursable Expenses are supported by

Supporting Documentation.

6.12 The Authority shall provide a copy of its current expenses policy to the Supplier upon request.

Promoting Tax Compliance

6.13 All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Authority shall, following the receipt of a valid VAT invoice, pay to the Supplier a sum equal to the VAT chargeable in respect of the Services.

6.14 The Supplier shall at all times comply with all other Laws and regulations relating to Tax.

6.15 The Supplier shall provide to the Authority name and, as applicable, the Value Added Tax registration number, PAYE collection number and either the Corporation Tax or self-assessment reference of any agent, supplier or sub-contractor of the Supplier prior to the commencement of any work under this Agreement by that agent, supplier or sub-contractor. Upon a justified written request by the Authority, the Supplier shall not employ or will cease to employ any agent, supplier or sub-contractor or sub-contractor.

6.16 Where an amount of Tax, including any assessed amount, is due from the Supplier an equivalent amount may be deducted by the Authority from the amount of any sum due to the Supplier under this Agreement.

6.17 If, at any point during the Term, an Occasion of Tax Non-Compliance occurs and or any litigation, enquiry or investigation in which it or its sub-contractors is/are (as appropriate) involved that is in connection with, or which may lead to, any Occasion of Tax Non-Compliance, the Supplier shall:

6.18 notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and

6.18.1 promptly provide to the Authority:

(a) details of the steps which the Supplier is taking to address the Occasion of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

(b) such other information in relation to the Occasion of Tax Non-Compliance as the Authority may reasonably require.

6.19 The Supplier shall indemnify the Authority against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any Tax relating to payments made to the Supplier under this Agreement. Any amounts due under this Clause 6.18 shall be paid in cleared funds by the Supplier to the Authority not less than five (5) Working Days before the date upon which the Tax or other liability is payable by the Authority.

6.20 The Supplier shall provide (promptly or within such other reasonable period notified in writing by the Authority) information which demonstrates how the Supplier complies with its Tax obligations.

6.21 If the Supplier fails to comply (or if the Authority receives information which demonstrates that the Supplier has failed to comply) with any of the provisions in Clauses 6.14 to 6.19 (inclusive) then this shall allow the Authority to terminate the Agreement pursuant to Clause 20.2.1 or Clause 20.2.3.

6.22 The Authority may internally share any information which it receives under Clauses 6.15 to 6.17 (inclusive) and 6.19.

Income Tax and National Insurance Contributions

6.23 Where the Supplier or any Supplier Personnel are liable to Tax in the UK or to pay national insurance contributions in respect of consideration received under this Agreement, the Supplier shall:

6.23.1 at all times comply with the Income Tax (Earnings and Pensions) Act 2003 and all other Laws and regulations relating to income tax, and the Social Security Contributions and Benefits Act 1992 and all other Laws and regulations relating to national insurance contributions, in respect of that consideration;

6.23.2 indemnify the Authority against any income tax, national insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the provision of the Services by the Supplier or any Supplier Personnel for which the Supplier is not primarily liable to account to the Authority under the relevant Laws and regulations; and

6.23.3 provide (promptly or within such other period notified by the Authority) information which demonstrates how the Supplier complies with Clause 6.22.1 or why Clause 6.22.1 does not apply to the Supplier (including such specific information as the Authority may request),

6.23.4 and if the Supplier fails to comply (or if the Authority receives information which demonstrates that the Supplier has failed to comply) with any of the provisions above in this Clause 6.22 then this shall allow the Authority to terminate the Agreement pursuant to Clause 20.2.1 or Clause 20.2.3..

6.24 The Authority may internally share any information which it receives under Clause 6.22.3.

7 Premises and equipment

7.1 If agreed between the Parties, and subject always to Clause 8, the Authority shall provide the Supplier with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Authority's premises by the Supplier or the Supplier Personnel shall be at the Supplier's risk.

7.2 If the Supplier supplies all or any of the Services at or from the Authority's premises, on completion of the Services or termination or expiry of the Agreement (whichever is the earlier) the Supplier shall vacate the Authority's premises, remove the Supplier's plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Authority's premises in a clean, safe and tidy condition. The Supplier shall be solely responsible for making good any damage to the Authority's premises or any objects contained on the Authority's premises which is caused by the Supplier or any Supplier Personnel, other than fair wear and tear.

7.3 If the Supplier supplies all or any of the Services at or from its premises or the premises of a third party, the Authority may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises.

7.4 The Authority shall be responsible for maintaining the security of its premises in

accordance with its standard security requirements. While on the Authority's premises the Supplier shall, and shall procure that all Supplier Personnel shall, comply with all the Authority's security requirements.

7.5 Where all or any of the Services are supplied from the Supplier's premises, the Supplier shall, at its own cost, comply with all security requirements of the Authority as notified to the Supplier from time to time in writing.

7.6 Without prejudice to Clause 2.2.6, any equipment provided by the Authority for the purposes of the Agreement shall remain the property of the Authority and shall be used by the Supplier and the Supplier Personnel only for the purpose of carrying out the Agreement. Such equipment shall be returned promptly to the Authority on expiry or termination of the Agreement.

7.7 The Supplier shall reimburse the Authority for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Supplier or any Supplier Personnel. Equipment supplied by the Authority shall be deemed to be in a good condition when received by the Supplier or relevant Supplier Personnel unless the Authority is notified otherwise in writing within 5 Working Days.

8 Supplier Personnel and Key Personnel

8.1 If the Authority reasonably believes that any of the Supplier Personnel are unsuitable to undertake work in respect of the Agreement, it may, by giving written notice to the Supplier:

8.1.1 refuse admission to the relevant person(s) to the Authority's premises;

8.1.2 direct the Supplier to end the involvement in the provision of the Services of the relevant person(s); and/or

8.1.3 require that the Supplier replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Authority to the person removed is surrendered,

and the Supplier shall comply with any such notice.

8.2 The Supplier shall:

8.2.1 ensure that all Supplier Personnel are vetted in accordance with good industry practice, BPSS and any security requirements set out in Schedule 1.1 (Services Description);

8.2.2 if requested, provide the Authority with a list of the names and addresses (and any other relevant information, including the capacities in which they are concerned with the Agreement) of all persons who may require admission to the Authority's premises in connection with the Agreement; and

8.2.3 procure that all Supplier Personnel comply with any rules, regulations and requirements reasonably specified in writing by the Authority.

8.3 Any 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, termination of employment or other extenuating circumstances.

8.4 Any replacements to the Key Personnel shall be subject to the prior written agreement of the Authority (not to be unreasonably withheld or delayed). 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. The Supplier shall use all reasonable endeavours to minimise any adverse

impact on the Agreement which could be caused by a change in Key Personnel.

8.5 Where Supplier Personnel are required to have a pass for admission to the Authority's premises, the Authority's representative shall, subject to satisfactory completion of approval procedures, arrange for passes to be issued.

9 Assignment and sub-contracting

9.1 The Supplier shall not without the prior written consent of the Authority assign, novate or in any way dispose of the benefit and/ or the burden of the Agreement or any part of the Agreement.

9.2 The Supplier shall not sub-contract any of its obligations under the Agreement without the prior written consent of the Authority, not to be unreasonably withheld of delayed. At the Authority's discretion, it may require the Supplier to provide information on the sub-contractor's identity, the services it is proposed to it will provide and any further information reasonably required to inform its decision, including a copy of the proposed sub-contract. The Supplier shall be responsible for the acts and omissions of its sub-contractors as though they are its own and shall include in each sub-contract provisions which will enable the Supplier to meet its obligations under the Agreement

9.3 The Authority may, in the granting of any consent pursuant to Clause 9.1 or 9.2, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Supplier shall be responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.

9.4 Where the Supplier enters into a sub-contract with a UK entity for the purpose of performing its obligations under the Agreement, it shall ensure that a provision is included in such sub-contract which requires payment to be made of all sums due by the Supplier to the sub-contractor within a specified period not exceeding 30 days from the receipt of a valid invoice.

9.5 Where the Authority has consented to the placing of sub-contracts, the Supplier shall, at the written request of the Authority, send copies of each sub-contract, to the Authority as soon as is reasonably practicable.

9.6 The Authority shall not assign, novate, or otherwise dispose any of its rights and obligations under the Agreement without the prior written consent of the Supplier not to be unreasonably withheld or delayed.

10 Intellectual Property Rights

10.1 All Intellectual Property Rights in any materials provided by the Authority to the Supplier for the purposes of this Agreement shall remain the property of the Authority but the Authority hereby grants the Supplier a royalty-free, non-exclusive and non-transferable licence to use such materials as required until termination or expiry of the Agreement for the sole purpose of enabling the Supplier to perform its obligations under the Agreement.

10.2 All Intellectual Property Rights in any materials created or developed by the Supplier pursuant to the Agreement or arising as a result of the provision of the Services shall vest in the Supplier. If, and to the extent, that any Intellectual Property Rights in such materials vest in the Authority by operation of law, the Authority hereby assigns to the Supplier by way of a present assignment of future rights that shall take place immediately on the coming into existence of any such Intellectual Property Rights all its Intellectual Property Rights in such materials (with full title guarantee and free from all

third party rights).

10.3 The Supplier hereby grants the Authority:

10.3.1 a perpetual, royalty-free, irrevocable, non-exclusive licence (with a right to sub-license) to use all Intellectual Property Rights in the materials created or developed pursuant to the Agreement and any Intellectual Property Rights arising as a result of the provision of the Services; and

10.3.2 a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:

(a) any Intellectual Property Rights vested in or licensed to the Supplier on the date of the Agreement; and

(b) any Intellectual Property Rights created during the Term but which are neither created or developed pursuant to the Agreement nor arise as a result of the provision of the Services,

including any modifications to or derivative versions of any such Intellectual Property Rights, which the Authority reasonably requires in order to exercise its rights and take the benefit of the Agreement including the Services provided.

10.4 The Supplier shall indemnify, and keep indemnified, the Authority in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees settled in accordance with the Dispute Resolution Process and/or finally awarded by an irrevocable court order against the Authority as a result of or in connection with any claim made against the Authority for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of the Supplier or any Supplier Personnel.

11 Remedies in the Event of Inadequate Performance

11.1 Where a complaint is received about the standard of service or about the way any Services have been delivered or work has been performed or about the Agreement or procedures used or about any other matter connected with the performance of this Agreement, then the Authority's contract manager shall take all reasonable steps to ascertain whether the complaint is valid.

11.2 In the event that the Authority considers there has been a breach of this Agreement by the Supplier, or the Supplier's performance of its duties under the Agreement has failed to meet the Authority's requirements, as set out in the Specification or otherwise in the Agreement, without prejudice to any other rights and remedies under the Agreement, the Authority may:

11.2.1 make such deduction as agreed between the Parties from the payment to be made to the Supplier to reflect sums paid or sums which would otherwise be payable in respect of such of the Services as the Supplier shall have either failed to provide or have provided inadequately or which the Supplier is not obliged to provide pursuant to Clause 11.2.

11.2.2 without terminating the Agreement, provide or procure the provision of part of the Services (and the Supplier shall not be obliged to provide such Services) until such time as the Supplier shall have demonstrated to the reasonable satisfaction of the Authority that the Supplier will once more be able to perform such part of the Services to the required standard;

11.2.3 without terminating the whole of the Agreement, terminate the Agreement in respect of part of the Services only (whereupon a corresponding reduction in the Charges shall be made) and thereafter itself provide or procure a third party to provide such part of the Services; and/or

11.2.4 terminate, in accordance with Clause 20, the whole of the Agreement.

12 Governance and Records

12.1 The Supplier shall:

12.1.1 attend progress meetings with the Authority at the frequency and times agreed between the Parties and shall ensure that its representatives are suitably qualified to attend such meetings; and

12.1.2 submit progress reports to the Authority at the times and in the format agreed between the Parties.

12.2 The Supplier shall keep and maintain until 6 years after the end of the Agreement, or as long a period as may be agreed between the Parties, full and accurate records of the Agreement including the Services supplied under it and all payments made by the Authority. The Supplier shall on request afford the Authority or the Authority's representatives such access to those records as may be reasonably requested by the Authority in connection with the Agreement.

13 Confidentiality, Transparency and Publicity

13.1 Subject to Clause 13.2, each Party shall:

13.1.1 treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and

13.1.2 not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Agreement.

13.2 Notwithstanding Clause 13.1, a Party may disclose Confidential Information which it receives from the other Party:

13.2.1 where disclosure is required by applicable law or by a court of competent jurisdiction;

13.2.2 to its auditors or for the purposes of regulatory requirements;

13.2.3 on a confidential basis, to its professional advisers;

13.2.4 to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;

13.2.5 where the receiving Party is the Supplier, to the Supplier Personnel on a need to know basis to enable performance of the Supplier's obligations under the Agreement provided that the Supplier shall procure that any Supplier Personnel to whom it discloses Confidential Information pursuant to this Clause 13.2.5 shall observe the Supplier's confidentiality obligations under the Agreement; and

13.2.6 where the receiving Party is the Authority:

(a) on a confidential basis to the employees, agents, consultants and contractors of the Authority;

(b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company to which the Authority transfers or proposes to transfer all or any part of its business;

(c) to the extent that the Authority (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or

(d) in accordance with Clause 15.

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Authority under this Clause 13.

13.3 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of the Agreement is not Confidential Information and the Supplier hereby gives its consent for the Authority to publish this Agreement in its entirety to the general public (but with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the Agreement agreed from time to time. The Authority may consult with the Supplier to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the provisions of the FOIA.

13.4 The Supplier shall not, and shall take reasonable steps to ensure that the Supplier Personnel shall not:

13.4.1 make any press announcement or publicise the Agreement or any part of the Agreement in any way; or

13.4.2 use the Authority's name or brand in any promotion or marketing or announcement of orders,

except with the prior written consent of the Authority.

13.5 Each Party acknowledges to the other that nothing in this Agreement either expressly or by implication constitutes an endorsement of any products or services of the other Party and each Party agrees not to conduct itself in such a way as to imply or express any such approval or endorsement.

13.6 The Supplier shall assist and cooperate with the Authority to enable the Authority to publish this Agreement.

14 Official Secrets Acts and related Legislation

14.1 The Supplier shall comply with, and shall ensure that it's Supplier Personnel comply with:

14.1.1 the provisions of the Official Secrets Acts 1911 to 1989;

14.1.2 the obligations set out in Section 182 of the Finance Act 1989 and Section 18 of the Commissioners for Revenue and Customs Act 2005 to maintain the confidentiality of Authority Data. Further, the Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the aforesaid obligations may lead to a prosecution under Section 182 of the Finance Act 1989 and/or Section 19 of the Commissioners for Revenue and

Customs Act 2005; and

14.1.3 Section 123 of the Social Security Administration Act 1992, which may apply to the fulfilment of some or all of the Services. The Supplier acknowledges that (without prejudice to any other rights and remedies of the Authority) a breach of the Supplier's obligations under Section 123 of the Social Security Administration Act 1992 may lead to a prosecution under that Act.

14.2 The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Personnel in writing of the obligations upon Supplier Personnel set out in Clause 14.1 above. The Supplier shall monitor the compliance by Supplier Personnel with such obligations.

14.3 The Supplier shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data sign (or have previously signed) a declaration, in a form acceptable to the Authority, acknowledging that they understand and have been informed about the application and effect of Section 18 and 19 of the Commissioners for Revenue and Customs Act 2005. The Supplier shall provide a copy of each such signed declaration to the Authority upon demand.

14.4 In the event that the Supplier or the Supplier Personnel fail to comply with this clause, the Authority reserves the right to terminate the Agreement under Clause 20.2.1 with immediate effect.

15 Freedom of Information

15.1 The Supplier acknowledges that the Authority is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall:

15.1.1 provide all necessary assistance and cooperation as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;

15.1.2 transfer to the Authority all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 5 Working Days of receipt;

15.1.3 provide the Authority with a copy of all Information belonging to the Authority requested in the Request for Information which is in its possession or control in the form that the Authority requires within 5 Working Days (or such other period as the Authority may reasonably specify) of the Authority's request for such Information; and

15.1.4 not respond directly to a Request for Information unless authorised in writing to do so by the Authority.

15.2 The Supplier acknowledges that the Authority may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Supplier or the Services (including commercially sensitive information) without consulting or obtaining consent from the Supplier. In these circumstances the Authority shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the Supplier advance notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

15.3 Notwithstanding any other provision in the Agreement, the Authority shall be responsible for determining in its absolute discretion whether any Information relating to the Supplier

or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.

16 Authority Data and Security Requirements

16.1 When handling Authority data (whether or not Personal Data), the Supplier shall ensure the security of the data is maintained in line with the security requirements of the Authority as notified to the Supplier from time to time in writing, including any requirements set out in Schedule 6 (Security Requirements).

16.2 Where the Authority is required to provide by e-mail to the Supplier or Supplier Personnel, any departmental or customer data or any other information with a security marking of "OFFICIAL-SENSITIVE", to enable it to deliver the Services, the Supplier shall not (and shall procure that the Supplier Personnel do not) store that information on its personal computer or any form of removable media.

16.3 Any breach of this Clause 16 may result in termination of the Agreement under Clause 20.2.

17 Liability

17.1 The Supplier shall not be responsible for any injury, loss, damage, cost or expense suffered by the Authority 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 Agreement.

17.2 Subject always to Clauses 17.3 and 17.3.2:

17.2.1 the Supplier's aggregate liability in respect of loss of or damage to the Authority premises or other property or assets of the Authority (including technical infrastructure, assets or equipment but excluding any loss or damage to the Authority's Data or any other data) that is caused by Defaults of the Supplier shall in no event exceed 1 million pounds;

17.2.2 the aggregate liability of the Supplier in respect of all other Losses howsoever caused, whether arising from breach of the Agreement, the supply or failure to supply of the Services, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed a sum equal to the 100% of the Charges paid or payable to the Supplier; and

17.2.3 except in the case of claims arising under Clauses 10.4 and 22.3, and subject to Clause 17.4, in no event shall the Supplier be liable to the Authority for any:

(a) loss of profits;

(b) loss of business;

(c) loss of revenue;

(d) loss of or damage to goodwill;

(e) loss of savings (whether anticipated or otherwise); and/or

(f) any indirect, special or consequential loss or damage.

17.3 Nothing in the Agreement shall be construed to limit or exclude:

17.3.1 either Party's liability for:

(a) death or personal injury caused by its negligence or that of the Supplier Personnel;

(b) fraud or fraudulent misrepresentation by it or that of the Supplier Personnel; or

(c) any other matter which, by law, may not be excluded or limited; or

17.3.2 the Supplier's liability under the indemnity in Clause 10.4 (*Intellectual Property Rights*) and 22.3 (*Prevention of Fraud and Corruption*); or

17.3.3 the Supplier's liability for any regulatory losses, fines and/or penalties incurred by the Authority and any further costs incurred by the Authority in order to meet any additional requirements imposed by a relevant regulatory body as a result of the relevant breach.

17.4 Notwithstanding Clause 17.2.3 but subject to Clause 17.2, the Supplier acknowledges that the Authority may, amongst other things, recover from the Supplier the following Losses incurred by the Authority to the extent that they arise as a result of a Default by the Supplier which are deemed to be a non-exhaustive list of direct and recoverable Losses:

17.4.1 the total amount of Tax Revenue which would have been collected and/or the total amount of any benefit or tax credit overpayment which would not have been made by or on behalf of the Authority had the Default not occurred;

17.4.2 notwithstanding Clauses 17.4.3 and 17.4.8, any operational and/or administrative costs and expenses incurred by the Authority in connection with dealing with a loss of Tax Revenue and/or any overpayment of any benefit or tax credit made as a result of a Default;

17.4.3 any additional operational and/or administrative costs and expenses incurred by the Authority, including costs relating to time spent by or on behalf of the Authority in dealing with the consequences of the Default;

17.4.4 any wasted expenditure or charges;

17.4.5 the additional cost of procuring Replacement Services for the remainder of the Term and/or replacement Deliverables, which shall include any incremental direct costs associated with such Replacement Services and/or replacement Deliverables above those which would have been payable under this Agreement;

17.4.6 any compensation or interest paid to a third party by the Authority;

17.4.7 any fine or penalty incurred by the Authority pursuant to Law and any costs incurred by the Authority in defending any proceedings which result in such fine or penalty; and

17.4.8 without prejudice to Clause 16 (Authority Data and Security Requirements), any losses associated with corruption, loss or degradation to Authority Data.

18 Insurance

18.1 The Supplier 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 Supplier, arising out of the Supplier's performance of its obligations under the Agreement, including in respect of 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 Supplier and shall be maintained for the Term.

18.2 The Supplier shall hold employer's liability insurance to a minimum of £5,000,000 in respect of Supplier Personnel in accordance with any legal requirement from time to time in force.

18.3 The Supplier 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.

18.4 The Supplier shall hold and maintain professional indemnity insurance cover and shall ensure that all professional contractors involved in the provision of the project hold and maintain appropriate cover. Such insurance to be held by the Supplier or by any agent or sub-contractor involved in the provision of the project may be limited in respect of any one claim (but shall not be limited in any other respect), provided that any such limit shall in any event be not less than £1,000,000 (one million pounds). Such insurance shall be maintained for a minimum of six years following expiration or earlier termination of this Agreement.

19 Force Majeure

19.1 Neither Party shall have any liability under or be deemed to be in breach of the Agreement for any delays or failures in performance of the Agreement which result from circumstances beyond the reasonable control of the Party affected. Each Party shall promptly notify the other Party in writing when such circumstances cause a delay or failure in performance and when they cease to do so. If such circumstances continue for a continuous period of more than two months, either Party may terminate the Agreement by written notice to the other Party.

20 Termination

20.1 The Authority may terminate the Agreement at any time by notice in writing to the Supplier to take effect on any date falling at least 3 months (or, if the Agreement is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.

20.2 Without prejudice to any other right or remedy it might have, the Authority may terminate the Agreement by written notice to the Supplier with immediate effect if the Supplier:

20.2.1 (without prejudice to Clause 20.2.5), is in material breach of any obligation under the Agreement which is not capable of remedy;

20.2.2 repeatedly breaches any of the terms and conditions of the Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Agreement;

20.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier receiving notice specifying the breach and requiring it to be remedied;

20.2.4 undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;

20.2.5 breaches any of the provisions of Clauses 8.2, 13, 15, 16 and 21; or

20.2.6 becomes insolvent, or if an order is made or a resolution is passed for the

winding up of the Supplier (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Supplier's assets or business, or if the Supplier makes any composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this Clause 20.2.6) in consequence of debt in any jurisdiction.

20.3 The Supplier shall notify the Authority as soon as practicable of any change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988.

20.4 The Supplier may terminate this Agreement by providing written notice to the Authority at any time by notice in writing to the Authority to take effect on any date falling at least 3 months (or, if the Agreement is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice:

20.4.1 if the Authority fails to pay an undisputed sum due to the Supplier under this Agreement and such amount remains outstanding thirty (30) days after the receipt by the Authority of a notice of non-payment from the Supplier or

20.4.2 if the Authority (without prejudice to breach by the Authority of Clause 13), is in material breach of any obligation under the Agreement which is not capable of remedy;

20.4.3 if the Authority repeatedly breaches any of the terms and conditions of the Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Agreement;

20.4.4 if the Authority is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier receiving notice specifying the breach and requiring it to be remedied.

20.5 Termination or expiry of the Agreement shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and Clauses 1, 2.2, 7.1, 7.2, 7.6, 7.7, 8, 10, 12.2, 13, 15, 16, 17, 20.6, 22.3, 23 and 24.7 or any other provision of the Agreement that either expressly or by implication has effect after termination.

20.6 Upon termination or expiry of the Agreement, the Supplier shall:

20.6.1 give all reasonable assistance to the Authority and any incoming supplier of the Services in accordance with schedule 6; and

20.6.2 return all requested documents, information and data to the Authority as soon as reasonably practicable.

21 Compliance

21.1 The Supplier shall comply with the requirements of the Health and Safety at Work etc. Act 1974 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Personnel and other persons working on the Authority's premises in the performance of its obligations under the Agreement.

21.2 The Supplier shall promptly notify the Authority of any health and safety hazards which may arise in connection with the performance of its obligations under the Agreement. The Authority shall promptly notify the Supplier of any health and safety hazards which may exist or arise at the Authority's premises and which may affect the Supplier in the performance of its obligations under the Agreement.

21.3 The Supplier shall:

21.3.1 comply with all the Authority's health and safety measures notified in writing to the Supplier while on the Authority's premises; and

21.3.2 notify the Authority immediately in the event of any incident occurring in the performance of its obligations under the Agreement on the Authority's premises where that incident causes any personal injury or damage to property which could give rise to personal injury.

21.4 The Supplier shall:

21.4.1 perform its obligations under the Agreement in accordance with all applicable equality Law and the Authority's equality and diversity policy as provided to the Supplier from time to time; and

21.4.2 take all reasonable steps to secure the observance of Clause 21.4.1 by all Supplier Personnel.

21.5 The Supplier shall supply the Services in accordance with the Authority's environmental policy as provided to the Supplier from time to time.

21.6 In performing its obligations under the Agreement, the Supplier shall;

(a) comply with all applicable anti-slavery and human trafficking laws, statutes, regulations from time to time in force including the Modern Slavery Act 2015;

(b) not engage in any activity, practice or conduct that would constitute an offence under sections 1, 2 or 4, of the Modern Slavery Act 2015; and

(c) notify the Authority as soon as it becomes aware, and in any event within five (5) working days, of any actual or suspected breach of its obligations under Clause 21.6(a) and/ or (b) including details of the breach and the mitigation action it has taken or intends to take in order to:

(i) remedy the breach; and

(ii) ensure future compliance with Clause 21.6(a) and (b).

21.7 If the Supplier fails to comply (or if the Authority receives information which demonstrates that the Supplier has failed to comply) with any of the provisions in Clause 21.6 then this shall allow the Authority to terminate the Agreement pursuant to Clause 20.2.1.

22 Prevention of Fraud and Corruption

22.1 The Supplier shall not offer, give, or agree to give anything, to any person 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 Agreement or for showing or refraining from showing favour or disfavour to any person in relation to the Agreement.

22.2 The Supplier shall take all reasonable steps, in accordance with good industry practice, to prevent fraud by the Supplier Personnel and the Supplier (including its shareholders, members and directors) in connection with the Agreement and shall notify the Authority immediately if it has reason to suspect that any fraud has occurred or is occurring or is likely to occur.

22.3 If the Supplier or the Supplier Personnel engages in conduct prohibited by Clause 22.1 or commits fraud in relation to the Agreement or any other contract with the Crown (including the Authority) the Authority may:

22.3.1 terminate the Agreement and recover from the Supplier 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 Agreement; or

22.3.2 recover in full from the Supplier any other loss sustained by the Authority in consequence of any breach of this Clause.

23 Dispute Resolution

23.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Agreement and such efforts shall involve the escalation of the dispute to the following sets of representatives consecutively:

23.1.1 first to the personnel listed as level 1 escalation point in Paragraph 4 (Contract Management Roles and Dispute Escalation Points) of Schedule 3 (Contract Management Plan and Management Information);

23.1.2 second to the personnel listed as level 2 escalation point in Paragraph 4 of Schedule 3;

23.1.3 thirdly to the personnel listed as level 3 escalation point in Paragraph 4 of Schedule 3;

23.1.4 finally, to the Authority's Chief Executive Officer and an appropriately senior representative of the Supplier,

provided that each set of representatives listed above shall consider the dispute for at least 10 Working Days before escalating the dispute to the next set of representatives listed above if the dispute remains unresolved and the Parties consider the matter sufficiently urgent to escalate.

23.2 If the dispute is not resolved by the Parties in accordance with Clause 23.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the "**Mediator**") chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.

23.3 If the Parties fail to appoint a Mediator within one month, or fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, either Party may exercise any remedy it has under applicable law.

23.4 Notwithstanding Clauses 23.1 to 23.3, either Party may at any time take proceedings or seek remedies before any court or tribunal of competent jurisdiction:

23.4.1 for interim or interlocutory remedies in relation to this Agreement or infringement by the other Party of that Party's Intellectual Property Rights; and/or

23.4.2 where compliance with Clause 23.1 to 23.3 may leave insufficient time for that Party to commence proceedings before the expiry of the limitation period.

24 General

24.1 Each of the Parties represents and warrants to the other that it has full capacity and authority, and all necessary consents, licences and permissions to enter into and perform its obligations under the Agreement, and that the Agreement is executed by its duly authorised representative.

24.2 A person who is not a party to the Agreement 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 the Parties.

24.3 The Agreement cannot be varied except in writing signed by a duly authorised representative of both the Parties.

24.4 The Agreement contains the whole agreement between the Parties and supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Agreement on the basis of any representation that is not expressly incorporated into the Agreement. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.

24.5 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Agreement shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Agreement.

24.6 The Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Agreement. Neither Party shall have, nor represent that it has, any authority to make any commitments on the other Party's behalf.

24.7 Except as otherwise expressly provided by the Agreement, all remedies available to either Party for breach of the Agreement (whether under the Agreement, statute or common law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.

24.8 If any provision of the Agreement is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Agreement and rendered ineffective as far as possible without modifying the remaining provisions of the Agreement, and shall not in any way affect any other circumstances of or the validity or enforcement of the Agreement.

25 Notices

25.1 Any notice to be given under the Agreement shall be in writing and may be served by personal delivery, first class recorded or, subject to Clause 25.3, e-mail to the address of the relevant Party set out in Paragraph 5 (Address for Notices) of Schedule 3 (Contract Management Plan and Management Information), or such other address as that Party may from time to time notify to the other Party in accordance with this clause.

25.2 Notices served as above shall be deemed served on the Working Day of delivery provided delivery is before 5.00pm on a Working Day. Otherwise, delivery shall be deemed to occur on the next Working Day. An email shall be deemed delivered when sent unless an error message is received.

25.3 Notices under Clauses 19 (Force Majeure) and 20 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in Clause 25.1.

26 Governing Law and Jurisdiction

26.1 The validity, construction and performance of the Agreement, and all contractual and

non-contractual matters arising out of it, shall be governed by English law and shall be subject to arbitration under the Rules of Arbitration of the London Court of International Arbitration (LCIA), by one (1) arbitrator appointed in accordance with the said Rules. The decision of the arbitration shall be binding over the Parties. Arbitration and shall be conducted in English language. The venue of arbitration shall be London, England.

SCHEDULE 1.1 SERVICES DESCRIPTION

HM REVENUE & CUSTOMS SERVICES DESCRIPTION	
A1. HMRC Information **Purchase Order to be issued under separate cover**	
CD Reference:	SR1253962880
Purchase / Limit Order No	To be populated post Contract Award
Material Group: For HMRC use only	To be populated post Contract Award
	HMRC Commercial Contact
Name: Contact Telephone No.: email:	[redacted]
	HMRC Work Manager
Name: Contact Telephone No.: Contact Address: email:	[redacted]
HMRC Authorised Officer: (Sponsor/Budget Approver/Invoicing & timesheets)	[redacted]

A2.	Supplier Information
Supplier:	NETCOMPANY UK LIMITED
Contact:	[redacted]
Contact Tel No:	[redacted]
Contact Address:	[redacted]
email:	[redacted]

A3.	Contractual Detail
Special Terms and Conditions: e.g., overtime, expenses, travel & subsistence, notice period.	See Schedule 1.1 - Annex 1 for HMRC Travel & Subsistence Policy

A4.	**Services Specification**
Service Title	New Computerised Transit System (NCTS) – Trader Testing Services
Primary Location: (including full address)	[redacted]
Services Start Date:	22/12/2022
End Date:	21/12/2023
Extension Options	The Authority may extend the Agreement for a period of up to 1 x 6 months
Contract Value	£4.5m

1. Definitions

"ERMIS"	ERMIS is a modular Commercial of the Shelf Customs solution developed by Netcompany.

2. Introduction

2.1. The Authority entered into contractual arrangement with the Supplier, under the reference 'SR666781155' on 11 May 2022, to deliver NCTS Phase 5. As part of this work, the Authority now require the Supplier to support in the wider activities associated with NCTS Phase 5 deployment.

2.2. The Authority require the Supplier, who currently deliver the NCTS Phase 5 ERMIS platform Transit component for both Great Britain (GB) and Northern Ireland (XI) NCTS services (otherwise referred to as "ERMIS") to provide additional support as follows:

2.2.1. Trader Testing/On-boarding & User training;

2.2.2. Additional NCTS Phase 5 development & deployment support; and

2.2.3. Testing support for the integrated service.

3. Statement of Works

3.1. Detailed implementation plan and statement of work(s) will be agreed between the Parties post contract award.

3.2. The statement of work(s) will provide detail of the activities and timeline required to ensure that the high-level deliverables (outlined in sections 3.3, 3.4 and 3.5) below, are executed successfully.

4. High-Level Deliverables

The Supplier is Responsible for delivering outcomes to time, quality, and cost against fixed price & outcomes-based statements of works for all changes.

The high-level Deliverables under this Contract can be split into three sections, as follows:

4.1. Trader Test/On-boarding & User training

HMRC require support from the Supplier in relation to Trader Test onboarding and User training, by delivering the following:

a. ERMIS-P5 Trader Test Helpdesk Training materials

b. ERMIS-P5 Trader Test Helpdesk Training environments

c. ERMIS-P5 Trader Test Helpdesk Training delivery

d. ERMIS-P5 Trader Test Helpdesk Resource augmentation for SME/high level technical support

e. Any Live support of ERMIS Live post-LID

The below table outlines key Trader Testing/On-boarding and user training activities, milestones, and the associated timeline. Further details will be agreed between the Buyer and Supplier via a statement of work, post contract:

Milestone/Deliverable/Activity	Timeline
Trader Testing/On-boarding and Helpdesk Support	
Provide Trader Test training materials such as Connectivity guides (B2B), Helpdesk manual (CWM) and Debugging manual	Dec 22 – March 23
Provide a detailed implementation and Trader Test plan	Dec 22
Deliver Trader helpdesk Readiness & Training	April 23 – May 23
Resolve issues via Debugging and Troubleshooting with Traders	May 23 – Nov 23
Provide weekly status reporting in relation to Trader on-boarding and completion of Test-cases	Dec 22 – Nov 23
Deliver Helpdesk support	May 23 - Nov 23
User training – Customs Officers/Operations/Business Admins/Super users	
Develop a detailed User Training Plan for Customs Officers/Business Admins & Super users	Jan 23
Develop and provide user training materials, such as User manual for Customs Officers and Business admins	Dec 22 – July 23
Conduct training sessions to support User Readiness	April 23 – Nov 23
Deliver training to and facilitate the continuous upskilling of Customs Officers/Operations/business Admins/ Super Users	June 23 – Nov 23
Provide monthly status reporting on User on-boarding and completion reports	Dec 22 – Nov 23

Further details in relation to the fixed price charges associated to the above milestones and deliverables is detailed in Schedule 1.2, 'Pricing'.

4.2. Additional development and deployment support

HMRC require the Supplier to deliver the following deliverables, which are not within scope under the existing contract 'SR666781155':

a. ERMIS operational DevOps person(s) to help with environment configuration & operation

b. Environment deployment support work to fix & avoid any blockers or delays to HMRC delivery

c. ensure ERMIS aligns with standards and processes

d. support team to get more rapid turnaround of queries & defects

The below table outlines key development support and environment support activities, milestones, and the associated timeline. Further details will be agreed between the Buyer and Supplier via a statement of work, post contract:

Milestones /Deliverables/Activity	Timeline
Development support	
Support the accelerated development of NCTS Phase 5	Dec 22 – May 23
Provide Project Management, weekly Status reporting and progress tracking.	Dec 22 – Nov 23
Provide support for bug fixing and technical clarifications	January 23 – May 23
Environment Support	
The provision of dedicated support for environment deployment, including all the current testing environments	Dec 22 – Nov 23
Deliver continuous support for HMRC DevOps	Dec 22 – Nov 23
Provide ongoing Training and collaboration with HMRC DevOps, to build capability in terms of 'training the trainer'	Dec 22 – Nov 23

Further details in relation to the fixed price charges associated to the above milestones and deliverables is detailed in Schedule 1.2, 'Pricing'.

4.3. Testing support

HMRC require the Supplier to deliver the following deliverables in relation to Testing support, which are not within scope under the existing contract 'SR666781155':

a. PVT Testers
b. Conformance Testing
c. Functional Test
d. Non Functional Test

The below table outlines key Testing support activities, milestones, and the associated timeline. Further details will be agreed between the Buyer and Supplier via a statement of work, post contract:

Milestones /Deliverables/Activity	Timeline
Conformance test	
Automating (what can be automated) of the conformance test	Dec 22 – July 23
Driving the planning, design and execution test of mode 0, 1, 2 and 3.	Dec 22 – Nov 23
Maintaining dialog with DG-TAXUD and weekly status reporting on progress	Dec 22 – July 23
Functional test	

Planning, designing, executing and reporting all functional tests of SIT, UAT, E2E, smoke and regression tests	Dec 22 – Nov 23
Non-functional test	
Planning, designing, executing and reporting all non-functional tests of PVT, OAT tests	Jan 23 – Nov 23

Further details in relation to the fixed price charges associated to the above milestones and deliverables is detailed in Schedule 1.2, 'Pricing'.

SCHEDULE 1.2 PRICING

1. Definitions

"ATP Milestone"	the Milestone linked to Authority to Proceed for the relevant Operational Services set out in the Implementation Plan included as part of future SoW's;
"CPP Milestone"	a contract performance point as set out in the Implementation Plan included as part of future SoW's, being the Milestone at which the Supplier has demonstrated that the Supplier Solution or relevant Service is working satisfactorily in its operating environment in accordance with Schedule 1.4 (Testing Procedures)
"Critical Service Failure"	is when: 1. There is a delay of 6 calendar months in the delivery of a non-critical Milestone included in a SoW, that is due to the fault of the Supplier, unless revised delivery dates have been agreed between the parties. 2. There is a delay of 3 calendar months in the delivery of a critical Milestone that is included in a SoW, that is due to the fault of the supplier, unless revised delivery dates have been agreed between the parties. 3. 15% Service Credits have been gained in more than 3 monthly reporting periods of any rolling 4-month period. 4. (warranty substitution) Where severity 1 or 2 fix SLAs have not been met for 3 consecutive months.
"Delay"	a. a delay in the Achievement of a Milestone by its Milestone Date; or b. delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan included as part of future SoW's;
"Delivery Delay Payments"	has the meaning given in Paragraphs 5.1 - 5.4 of Schedule 1.2 Pricing
"Milestone"	an event or task described in the Implementation Plan included as part of future SoW's which, if applicable, shall be completed by the relevant Milestone Date;

"Deliverable"	an item or feature delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Agreement;
"Implementation Plan"	A detailed plan to document milestone activities and target delivery dates, included as part of future SoW's.
"Milestone Achievement Certificate"	the certificate to be granted by the Authority when the Supplier has Achieved a Milestone, which shall be in substantially the same form as that set out in the SoW;
"Milestone Date"	the target date set out against the relevant Milestone in the Implementation Plan included as part of future SoW's by which the Milestone must be Achieved;
"Milestone Payment"	a payment identified in the Statement of Work to be made following the issue of a Milestone Achievement Certificate
"Milestone Retention"	has the meaning given in Paragraph 4.3 of Schedule 1.2 Pricing
"Operational Services"	the operational services described as such in Schedule 1.1 (Services Description);
"Service Charges"	the periodic payments made in accordance with Schedule 1.2 (Pricing) in respect of the supply of the Operational Services;
"Statement of Work", SoW	a document signed by the Authority and Supplier describing a specific set of activities and/or Deliverables which the Supplier is to provide the Authority, issued pursuant to this Agreement. This document will include the Supplier's charges and how they will meet the Authority's requirements.
"Supporting Documentation	sufficient information in writing to enable the Authority reasonably to assess whether the Charges, Reimbursable Expenses and other sums due from the Authority detailed in the information are properly payable, including copies of any applicable Milestone Achievement Certificates or receipts;

2. Applicable Pricing Mechanism

2.1. Service Charges shall be calculated using the pricing mechanism specified in in this Schedule and on the basis of the rates and prices specified in Annex 1.

3. Professional Services Charging approach

3.1. All changes to the Service's will be managed through "Change Requests" in accordance with Schedule 4 Change Control Procedure.

3.2. Changes Requests that require changes to the Supplier's solution will be managed through Statements of Work. The Milestones Payment will be calculated by reference to the following pricing mechanism:

2.2.1 The day rates set out in Annex 1 shall be used to calculate the relevant Charges, provided that the Supplier (or its Sub-contractor) shall:

a) unless otherwise agreed by the Authority the Supplier's proposals will include fixed price Charges for each Milestone;

b) demonstrate how their Charges have been calculated:

c) not be entitled to include any uplift for risks or contingencies within its day rates;

d) where the authority has agreed time and material, only be entitled to be paid Charges that have been properly and reasonably incurred, taking into account the Supplier's obligation to deliver the Services in a proportionate and efficient manner; and

e) keep records of hours properly worked by Supplier Personnel (in the form of timesheets) and expenses incurred and submit a summary of the relevant records with each invoice. If the Authority requests copies of such records, the Supplier shall make them available to the Authority within 10 Working Days of the Authority's request.

4. Milestone Payments

4.1. Subject to the provisions of Paragraph 5 in relation to the deduction of Delivery Delay Payments, on the Achievement of a Milestone the Supplier shall be entitled to invoice the Authority for the Milestone Payment associated with that Milestone less the applicable Milestone Retention in accordance with this Schedule.

4.2. Each invoice relating to a Milestone Payment shall be supported by:

a) a Milestone Achievement Certificate; and

b) where the Milestone Payment is to be calculated by reference Time and Materials pricing mechanism, the supplier will provide Supporting Documentation.

4.3. The "Milestone Retention" for each Milestone determined by reference to a Time and Materials or Fixed Price pricing mechanism, 10% of the Charges for that Milestone,

and prior to deduction from the Milestone Payment of any Delay Payment attributable to that Milestone and without taking account of any amount payable by the Supplier pursuant to Section 5.

5. Delivery Delay Payments

5.1. The Customer will categorise Milestones as critical or non-critical within future SoW's. Each Milestone will be categorised on a case-by-case basis, taking into account impact on wider NCTS delivery/performance and value (e.g., less than £200K excluding VAT).

5.2. In the event of failure to deliver a non-critical fixed price Milestone, that is due to the fault of the Supplier, the Supplier will be required to complete the work at its own cost and the relevant payment for that Milestone will be withheld until completion and acceptance. The following other measures will immediately be put in place:

4.2.1 The Supplier will issue a delay notice in advance or exceptionally on the milestone date, setting out the reasons for delay. A single Supplier owner for resolution will be appointed.

4.2.2 The Supplier will share a mitigation plan with the Authority within 3 working days of a missed Milestone.

4.2.3 Regular reporting will be put in place with the Authority's point of contact until the Milestone has been met.

4.2.4 In the event that the Milestone has still not been met within two months of the original milestone date, a delay penalty of 5% of the Milestone value will apply.

4.2.5 In the event that the Milestone has still not been met six months after the original milestone date, the Authority will have the right to invoke a Critical Service Failure event and issue a termination notice to the Supplier.

5.3. In the event of failure to deliver a critical fixed price Milestone, that is due to the fault of the Supplier, the Supplier will be required to complete the work at its own cost and the relevant payment for that milestone will be withheld until completion and acceptance. The following other measures will immediately be put in place:

4.3.1 The Supplier will issue a delay notice in advance or exceptionally on the Milestone date setting out the reasons for delay. A single Supplier owner for resolution will be appointed.

4.3.2 The Supplier will share a mitigation plan with the Authority within 5 working days of a missed Milestone.

4.3.3 Regular reporting will be put in place with the Authority point of contact until the Milestone has been met.

4.3.4 The Supplier's will make its Account Manager available to discuss the issue and understand the plan to fix.

4.3.5 In the event that the Milestone has still not been met within one month of the original Milestone date, a delay penalty of 5% of the Milestone value will apply.

4.3.6 In the event that the Milestone has still not been met within two months of the original Milestone date, a second delay penalty of 5% of the Milestone value will apply. This is in addition to the delay penalty in clause 4.3.5 above.

4.3.7 In the event that the Milestone has still not been met three months after the original milestone date, the Authority will have the right to invoke a Critical Service Failure event and issue a termination notice to the Supplier.

5.4. In the event that that a delay occurs that is not the fault of the Supplier (e.g., because the Customer has missed a key dependency), the Supplier should issue a delay notice as soon as it becomes aware of the issue, citing the reason, indicating the period of delay and requesting joint agreement to a revised schedule and if necessary additional charges. The Customer cannot reasonably withhold agreement.

6. Release of Milestone Retention

6.1. On Achievement of a CPP Milestone relating to the Supplier Solution or one or more Services (as the case may be), the Supplier shall be entitled to invoice the Authority for an amount equal to all Milestone Retentions that relate to Milestones identified in the "CPP Milestone Charge Number" column of Table 1 (or, in relation to Milestone Retentions in respect of Optional Services, Table 4) of Annex 2 and corresponding CPP Milestone Charge Number identified in Table 2 of Annex 4 of Schedule 1.4 (Testing Procedures) as being payable in respect of that CPP Milestone and have not been paid before such CPP Milestone

ANNEX 1: PRICING MECHANISM

1. Contract Value

1.1. The total value of the 1 year term of the contract is £4.5M, excluding VAT.

1.2. Professional services for NCTS Trader Support Window are going to be delivered under a fixed price arrangement, for a total value of £4.1M.

1.3. Further details of the fixed price breakdown against each of the three high-level deliverables, can be found within the tables at section(s) 1.2, 1.3 and 1.4, below.

1.4. For clarity:

1.4.1. 'Onshore' pricing will be applicable for any Supplier resource, deployed under this contract, who is based within either the UK or Denmark.

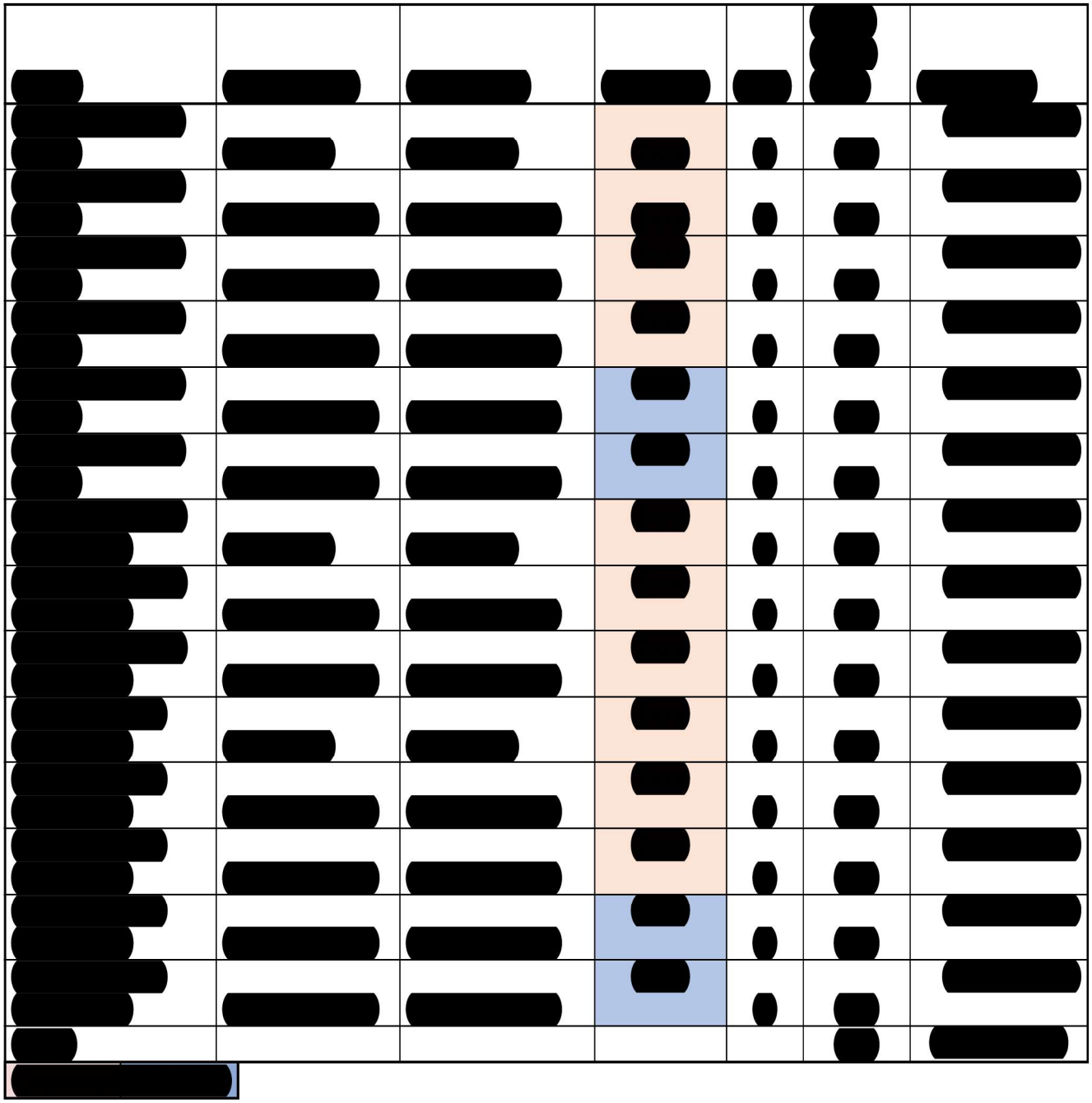
1.4.2. 'Offshore' pricing will be applicable for any Supplier resource, deployed under this contract, who is based in any other location outside of the UK, other than Denmark.

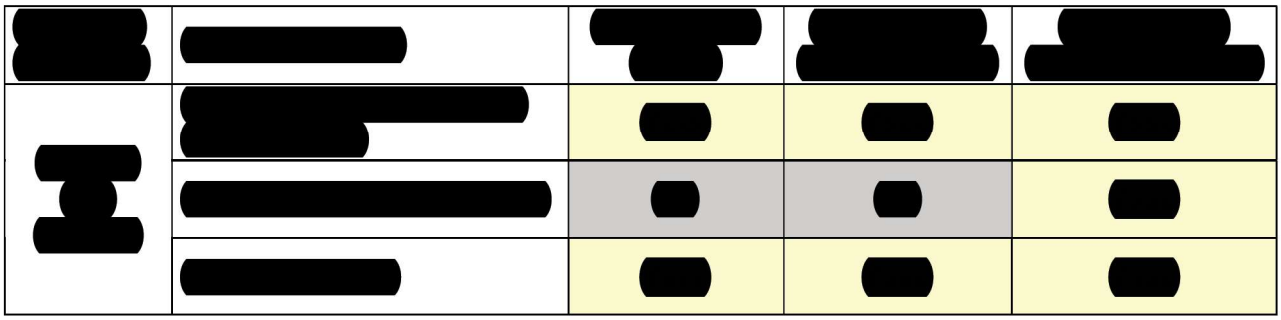
[redacted]

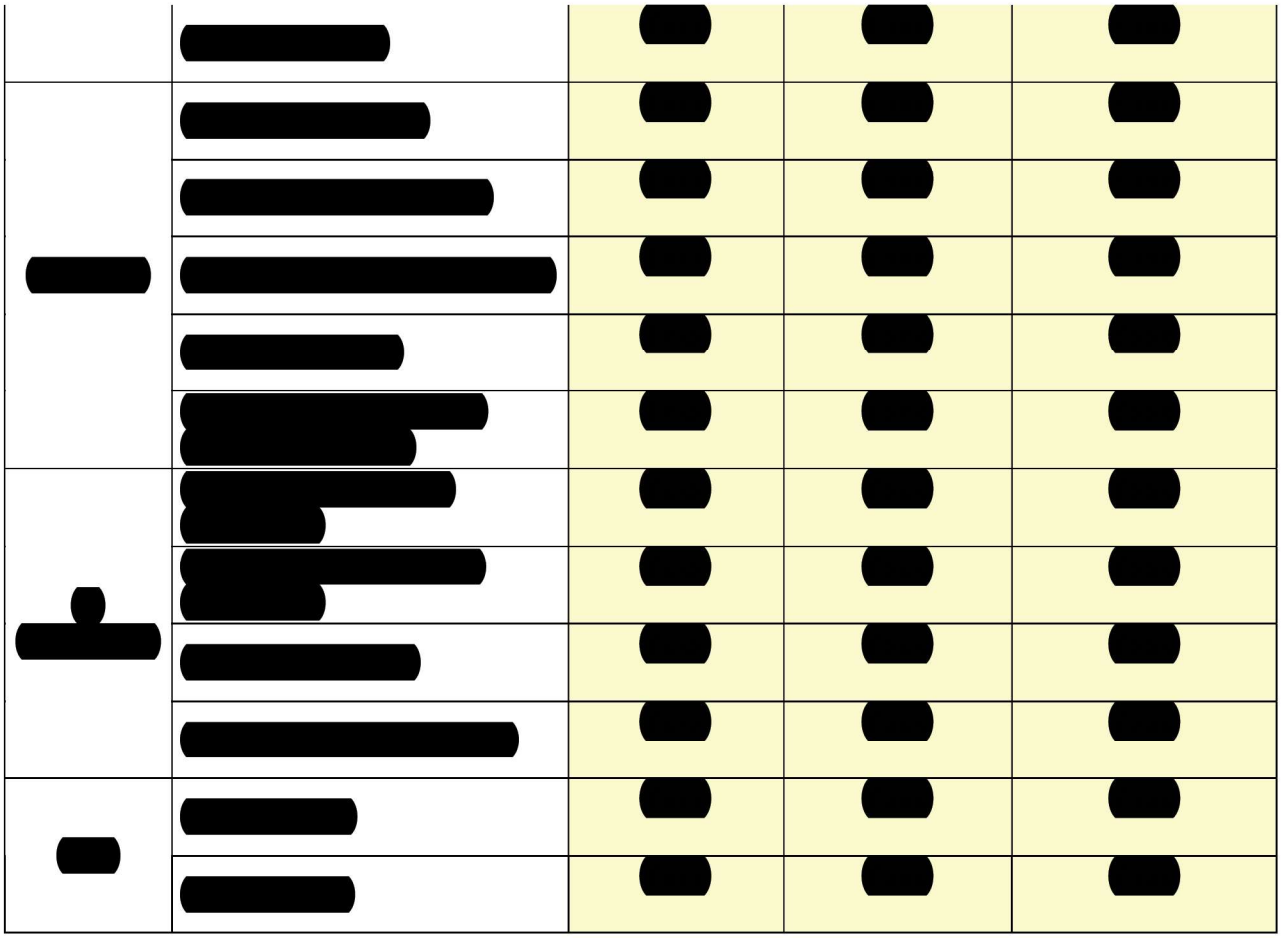
[redacted]

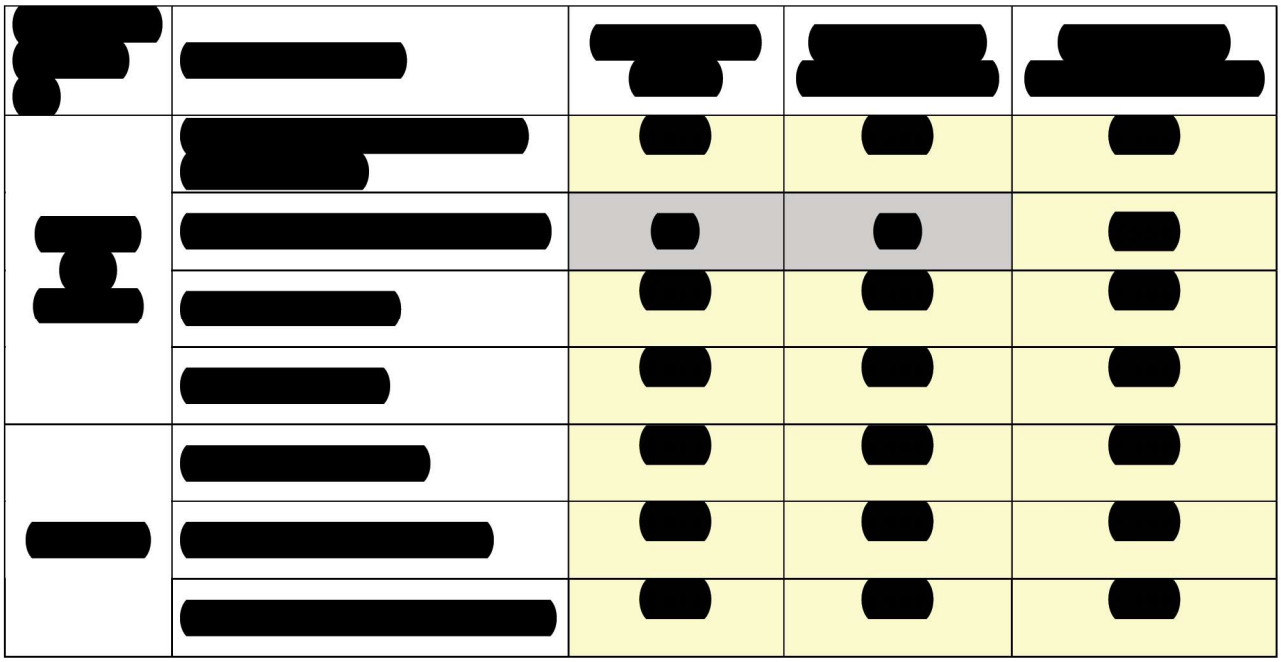
[redacted]

[redacted]









[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]

ANNEX 1 HMRC TRAVEL & SUBSISTENCE POLICY

HMRC Policy

HMRC Sustainable travel policy

HMRC is committed to adopting more sustainable travel behaviours. Travel plays an important role in delivering many aspects of our business, but travel can also have a negative impact on the environment and on your work life balance. We are working to improve our travel management so that we can contribute to the Government's Sustainable Development Objectives. This will help reduce the impact of climate change.

How you can help deliver our business sustainably

You can help in two straightforward ways:

Avoid travelling in the first place. This is about minimising your need to travel to meet your business objectives. You can change your working practices and help develop a culture which supports not travelling.

For meetings your starting point should be that the meeting can be delivered effectively remotely. If you are responsible for setting up meetings you should take the lead on this. If meeting attendees, ask to use remote communication methods you should do all you can to achieve this.

Travel for business can be essential in certain circumstances. Before you travel or ask others to travel on official business, you must decide whether your business objective can be achieved using alternatives. A well-run teleconference / Teams meeting can be as effective as a face to face meeting. It also saves 95% of the cost in expenses and staff time spent travelling.

If you must travel, **use more sustainable modes of transport**. Train, tube and bus are the most sustainable options.

Face to face meetings should be set up in locations with public transport access wherever possible.

Before you organise and undertake any travel you must have a clear business justification for your journey and obtain prior approval from your contract manager. Your manager will make clear, as part of your team's business planning, when travel is appropriate and when alternative working options should be applied.

It's your responsibility to agree with your contract manager **before you travel that you are intending using** the most cost effective, practical and sustainable travel option and **that budget is in place to cover the cost to travel**

Claiming expenses

Claim only what you are entitled to claim in accordance with the T&S guidance below.

Make sure you have receipts to support your claims as these are important in ensuring that HMRC achieves the same standards of record keeping as for its own staff and its contractors as HMRC expects of other taxpayers.

Maintain your own personal record of expenses incurred as additional support to your claims

Make sure you submit any claims within three months of the date the expenses are incurred, as this allows managers and budget holders to manage their resources more effectively.

Only claim T&S for your meals and travel only, do not claim any element of T&S for your colleague's meal or travel as this may attract potential tax implication.

A process for claims should be agreed with your contract manager at the start of the contract

Your contract Manager will refuse to pay any claims above the stated rates

Your contract manager can refuse to pay any claim where the Policy has not been met

All HMRC T&S claims are subject to audit and public scrutiny

Journeys you can and can't claim for

If you make	then
a journey while you are on official business	you can claim for this journey.
a journey between your home and your designated workplace	you can't claim for this journey

Class of travel by Rail

Use **standard class travel for all rail journeys** irrespective of the journey time, unless you fulfil the conditions to travel first class (see below).

If you have your manager's approval before the journey takes place, and if	then
you have special needs that require you to travel at a higher class	you may travel first class.
there is a business need for you to travel with a colleague who may travel first class	you may travel first class.
the cost of first-class travel is cheaper or the same cost as standard class travel	you may travel first class.

Class of travel by Air

All staff should use economy class travel for flights of 2.5 hours or less, but you may travel premium economy or business class by air if either:

the flight exceeds 2.5 hours

no economy seats are available for flights of 2.5 hours or less.

Exceptionally, you may travel first class if premium economy or business class seats are not available on a specific flight exceeding 2.5 hours that you need to catch.

Mileage allowances

Allowance	Rate (pence per mile)
Higher Rate Mileage Allowance (limited to the first 10,000 miles in any financial year)	45p
Basic Rate Mileage Allowance	25p
Motorcycle Rate	24p
Pedal Cycle Rate	20p

Day Subsistence rates

Provided you incur a cost that is **more** than you would normally have incurred at home or your office, actual expenditure will be paid within these limits:

Allowance	Details	Amount
One Meal Allowance	Where away from home and permanent workplace for more than 5 hours	up to a maximum of £8.25
Two Meal Allowance	Where away from home and permanent workplace for more than 10 hours	up to a maximum of £17.75
Three Meal Allowance	Where away from home and permanent workplace for more than 13 hours	up to a maximum of £26.00
Unplanned late working	Where you must buy a meal when you are unexpectedly required to work after 20:00 hours in addition to your normal day **and** more than 3 hours after the end of your normal day	up to a maximum of £8.25

Short-term Night Subsistence Allowances

Hotel Bed and Breakfast Capped Rates

At the following locations, **actual** expenditure incurred within these limits.

Location	Hotel B&B capped limit:
London / within M25 (excluding Heathrow Airport)	£130
Bristol; Heathrow Airport	£100
Oxford; Portsmouth	£95
Elsewhere in UK	£90

Hotel rates can be higher during peak times, so contract managers can consider requests to exceed the capped rate, particularly if there are any personal safety concerns with the location of a cheaper rate hotel.

Short-term Overnight Subsistence Allowances

Allowance	Detail	Amount
Main Meal Allowance -	Actual expenditure on an evening meal if away overnight	up to a maximum of £26.00 for each night
Travel from Hotel to Detached Duty Office	Actual costs subject to reasonable value-for-money/business considerations	VFM
Staying with Family or Friends Allowance	You choose to stay with family or friends instead of at a hotel	£25.00 per night.
Personal Expenses Allowance -	actual cost of unavoidable personal expenses incurred	up to maximum of £5 for each night

Expenses for journeys you can't claim

If	then
your vehicle does not meet HMRC's insurance requirements; Business user is included	you can't claim mileage allowance.

If	then
expenses have been paid to you or are due to be paid to you by a third party - for example, another government department or organisation	you can't claim.
you incur parking penalties or fines for motoring offences	you can't claim.
you incur parking excess charges	you can't claim

SCHEDULE 1.3 IMPLEMENTATION PLAN

Capitalised terms used in this Schedule have the meanings given to them in the Terms & Conditions or Schedule 1.2 (Pricing) of the Agreement.

1 Introduction

1.1. This Schedule:

(a) defines the process for the preparation and implementation of the Outline Implementation Plan and Detailed Implementation Plan; and

(b) identifies the Milestones (and associated Deliverables) including the Milestones which trigger payment to the Supplier of the applicable Milestone Payments following the issue of the applicable Milestone Achievement Certificate.

2 Outline Implementation Plan

2.1 An Outline Implementation Plan, which will contain detail around Milestones to be delivered, will be included within each individual future SoW(s).

2.2 All changes to the Outline Implementation Plan shall be subject to the Change Control Procedure provided that the Supplier shall not attempt to postpone any

of the Milestones using the Change Control Procedure or otherwise (except in accordance with Clause 31 (Authority Cause)).

3 Approval Of The Detailed Implementation Plan

3.1 The Supplier shall submit a Detailed Implementation Plan to the Authority for approval within 10 Working Days of the Authority issuing a SoW for proposal to the Supplier.

3.2 The Supplier shall ensure that the draft Detailed Implementation Plan:

(a) incorporates all of the Milestones and Milestone Dates in order to achieve the deliverables set out within the SoW;

(b) includes the Supplier's proposed timescales for each of the Milestones detailed within the SoW:

(c) clearly outlines all the steps required to implement the Milestones to be achieved, in conformity with the Authority Requirements;

(d) clearly outlines the required roles and responsibilities of both Parties, including staffing requirements; and

(e) is produced using a software tool as specified, or agreed by the Authority.

3.3 Prior to the submission of the draft Detailed Implementation Plan to the Authority in accordance with Paragraph 3.1, the Authority shall have the right:

(a) to review any documentation produced by the Supplier in relation to the development of the Detailed Implementation Plan, including:

(i) details of the Supplier's intended approach to the Detailed Implementation Plan and its development;

(ii) copies of any drafts of the Detailed Implementation Plan produced by the Supplier; and

(iii) any other work in progress in relation to the Detailed Implementation Plan; and

(b) to require the Supplier to include any reasonable changes or provisions in the Detailed Implementation Plan.

3.4 Following receipt of the draft Detailed Implementation Plan from the Supplier, the Authority shall:

(a) review and comment on the draft Detailed Implementation Plan as soon as reasonably practicable; and

(b) notify the Supplier in writing that it approves or rejects the draft Detailed Implementation Plan no later than 20 Working Days after the date on which the draft Detailed Implementation Plan is first delivered to the Authority.

3.5 If the Authority rejects the draft Detailed Implementation Plan:

(a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and

(b) the Supplier shall then revise the draft Detailed Implementation Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft Detailed Implementation Plan to the Authority for the Authority's approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 3.4 and this Paragraph 3.5 shall apply again to any resubmitted draft Detailed Implementation Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

3.6 If the Authority approves the draft Detailed Implementation Plan, it shall replace the Outline Implementation Plan from the date of the Authority's notice of approval.

4 Updates To And Maintenance Of The Detailed Implementation Plan

4.1 Following the approval of the Detailed Implementation Plan by the Authority:

(a) the Supplier shall submit a revised Detailed Implementation Plan to the Authority to reflect any changes to the original Detailed Implementation Plan.

(b) without prejudice to Paragraph 4.1(a), the Authority shall be entitled to request a revised Detailed Implementation Plan at any time by giving written notice to the Supplier and the Supplier shall submit a draft revised Detailed Implementation Plan to the Authority within 20 Working Days of receiving such a request from the Authority (or such longer period as the Parties may agree provided that any failure to agree such longer period shall be referred to the Dispute Resolution Procedure);

(c) any revised Detailed Implementation Plan shall (subject to Paragraph 4.2) be submitted by the Supplier for approval in accordance with the procedure set out in Paragraph 3; and

(d) the Supplier's performance against the Implementation Plan shall be monitored at meetings of the Service Management Board (as defined in Schedule 8 (Governance). In preparation for such meetings, the current Detailed Implementation Plan shall be provided by the Supplier to the Authority not less than 5 Working Days in advance of each meeting of the Service Management Board.

4.2 Save for any amendments which are of a type identified and notified by the Authority (at the Authority's discretion) to the Supplier in writing as not requiring

approval, any material amendments to the Detailed Implementation Plan shall be subject to the Change Control Procedure provided that:

(a) any amendments to elements of the Detailed Implementation Plan which are based on the contents of the Outline Implementation Plan shall be deemed to be material amendments; and

(b) in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date except in accordance with Clause 31 (Authority Cause).

4.3 Any proposed amendments to the Detailed Implementation Plan shall not come into force until they have been approved in writing by the Authority.

5 GOVERNMENT REVIEWS

5.1 The Supplier acknowledges that the Services may be subject to Government review at key stages of the project. The Supplier shall cooperate with any bodies undertaking such review and shall allow for such reasonable assistance as may be required for this purpose within the Charges.

ANNEX 1: OUTLINE IMPLEMENTATION PLAN

1 Acceptance Milestones:

1.1 Acceptance Criteria will be formed, stated, and from both parts agreed, in alignment with the milestones within each SoW

2 Payment Schedule:

2.1 The payment schedule will be agreed within each individual SoW.

SCHEDULE 1.4 TESTING PROCEDURES

1 Definitions

In this Schedule, the following definitions shall apply:

"Component"	any constituent parts of the infrastructure for a Service, hardware or Software;
"Material Test Issue"	a Test Issue of Severity Level 1 or Severity Level 2;
"Severity Level"	the level of severity of a Test Issue, the criteria for which are described in Annex 1;
"Test Certificate"	a certificate materially in the form of the document contained in Annex 2 issued by the Authority when a Deliverable has satisfied its relevant Test Success Criteria;
"Test Issue"	any variance or non-conformity of a Deliverable from its requirements (such requirements being set out in the relevant Test Success Criteria);
"Test Issue Threshold"	in relation to the Tests applicable to a Milestone, a maximum number of Severity Level 3, Severity Level 4 and Severity Level 5 Test Issues as set out in the relevant Test Plan;
"Test Issue Management Log"	a log for the recording of Test Issues as described further in Paragraph 9.1
"Test Plan"	a plan: (a) for the Testing of Deliverables; and (b) setting out other agreed criteria related to the achievement of Milestones, as described further in Paragraph 5;
"Test Reports"	the reports to be produced by the Supplier setting out the results of Tests;
"Test Specification"	the specification that sets out how Tests will demonstrate that the Test Success Criteria have been satisfied, as described in more detail in Paragraph 7;
"Test Success Criteria"	in relation to a Test, the test success criteria for that Test as referred to in Paragraph 6;
"Test Witness"	any person appointed by the Authority pursuant to Paragraph 10.1; and
"Testing Procedures"	the applicable testing procedures and Test Success Criteria set out in this Schedule.

Capitalised terms used in this Schedule have the meanings given to them in this Schedule, Terms & Conditions or Schedule 1.2 (Pricing) of the Agreement.

2 Risk

2.1 The issue of a Test Certificate, a Milestone Achievement Certificate and/or a conditional Milestone Achievement Certificate shall not:

(a) operate to transfer any risk that the relevant Deliverable or Milestone is complete or will meet and/or satisfy the Authority's requirements for that Deliverable or Milestone; or

(b) affect the Authority's right subsequently to reject:

(i) all or any element of the Deliverables to which a Test Certificate relates; or

(ii) any Milestone to which the Milestone Achievement Certificate relates.

2.2 Notwithstanding the issuing of any Milestone Achievement Certificate (including the Milestone Achievement Certificate in respect of Authority to Proceed), the Supplier shall remain solely responsible for ensuring that:

(a) the Supplier Solution as designed and developed is suitable for the delivery of the Services and meets the Authority Requirements;

(b) the Services are implemented in accordance with this Agreement; and

(c) each Target Performance Level is met from the relevant Operational Service Commencement Date.

3 Testing Overview

3.1 All Tests conducted by the Supplier shall be conducted in accordance with the Test Strategy, the Test Plans and the Test Specifications.

3.2 The Supplier shall not submit any Deliverable for Testing:

(a) unless the Supplier is reasonably confident that it will satisfy the relevant Test Success Criteria;

(b) until the Authority has issued a Test Certificate in respect of any prior, dependant Deliverable(s); and

(c) until the Parties have agreed the Test Plan and the Test Specification relating to the relevant Deliverable(s).

3.3 The Supplier shall use reasonable endeavours to submit each Deliverable for Testing or re-Testing by or before the date set out in the Implementation Plan for the commencement of Testing in respect of the relevant Deliverable.

3.4 Prior to the issue of a Test Certificate, the Authority shall be entitled to review the relevant Test Reports and the Test Issue Management Log.

3.5 Any Disputes between the Authority and the Supplier regarding Testing shall be referred to

4 Test Strategy

4.1 The Supplier shall develop the final Test Strategy as soon as practicable after the Effective Date but in any case no later than 20 Working Days (or such other period as the Parties may agree in writing) after the Effective Date.

4.2 The final Test Strategy shall include:

(a) an overview of how Testing will be conducted in accordance with the Implementation Plan;

(b) the process to be used to capture and record Test results and the categorisation of Test Issues;

(c) the method for mapping the expected Test results to the Test Success Criteria;

(d) the procedure to be followed if a Deliverable fails to satisfy the Test Success Criteria or produces unexpected results, including a procedure for the resolution of Test Issues;

(e) the procedure to be followed to sign off each Test;

(f) the process for the production and maintenance of Test Reports and reporting, including templates for the Test Reports and the Test Issue Management Log, and a sample plan for the resolution of Test Issues;

(g) the names and contact details of the Authority's and the Supplier's Test representatives;

(h) a high level identification of the resources required for Testing, including facilities, infrastructure, personnel and Authority and/or third party involvement in the conduct of the Tests;

(i) the technical environments required to support the Tests; and

(j) the procedure for managing the configuration of the Test environments.

5 Test Plans

5.1 The Supplier shall develop Test Plans and submit these for the approval of the Authority as soon as practicable but in any case no later than 20 Working Days (or such other period as the Parties may agree in the Test Strategy or otherwise

agree in writing) prior to the start date for the relevant Testing (as specified in the implementation Plan).

5.2 Each Test Plan shall include as a minimum:

(a) the relevant Test definition and the purpose of the Test, the Milestone to which it relates, the requirements being tested and, for each Test, the specific Test Success Criteria to be satisfied;

(b) a detailed procedure for the Tests to be carried out, including:

(i) the timetable for the Tests, including start and end dates;

(ii) the Testing mechanism;

(iii) dates and methods by which the Authority can inspect Test results or witness the Tests in order to establish that the Test Success Criteria have been met;

(iv) the mechanism for ensuring the quality, completeness and relevance of the Tests;

(v) the format and an example of Test progress reports and the process with which the Authority accesses daily Test schedules;

(vi) the process which the Authority will use to review Test Issues and the Supplier's progress in resolving these in a timely basis;

(vii) the Test Schedule;

(viii) the re-Test procedure, the timetable and the resources which would be required for re-Testing; and

(c) the process for escalating Test Issues from a re-test situation to the taking of specific remedial action to resolve the Test Issue.

5.3 The Authority shall not unreasonably withhold or delay its approval of the Test Plans provided that the Supplier shall incorporate any reasonable requirements of the Authority in the Test Plans.

6 Test Success Criteria

The Test Success Criteria for:

(a) each Test that must be Achieved for the Supplier to Achieve either the ATP Milestone or a CPP Milestone are set out in Annex 4; and

(b) all other Tests shall be agreed between the Parties as part of the relevant Test Plan pursuant to Paragraph 5.

7 Test Specification

7.1 Following approval of a Test Plan, the Supplier shall develop the Test Specification for the relevant Deliverables as soon as reasonably practicable and in any event at least 10 Working Days (or such other period as the Parties

may agree in the Test Strategy or otherwise agree in writing) prior to the start of the relevant Testing (as specified in the Implementation Plan).

7.2 Each Test Specification shall include as a minimum:

(a) the specification of the Test data, including its source, scope, volume and management, a request (if applicable) for relevant Test data to be provided by the Authority and the extent to which it is equivalent to live operational data;

(b) a plan to make the resources available for Testing;

(c) Test scripts;

(d) Test pre-requisites and the mechanism for measuring them; and

(e) (expected Test results, including:

(i) a mechanism to be used to capture and record Test results; and

(ii) a method to process the Test results to establish their content.

8 Testing

8.1 Before submitting any Deliverables for Testing the Supplier shall subject the relevant Deliverables to its own internal quality control measures.

8.2 The Supplier shall manage the progress of Testing in accordance with the relevant Test Plan and shall carry out the Tests in accordance with the relevant Test Specification. Tests may be witnessed by the Test Witnesses in accordance with Paragraph 10.

8.3 The Supplier shall notify the Authority at least 10 Working Days (or such other period as the Parties may agree in writing) in advance of the date, time and location of the relevant Tests and the Authority shall ensure that the Test

Witnesses attend the Tests, except where the Authority has specified in writing that such attendance is not necessary.

8.4 The Authority may raise and close Test Issues during the Test witnessing process.

8.5 The Supplier shall provide to the Authority in relation to each Test

(a) a draft Test Report not less than 2 Working Days (or such other period as the Parties may agree in writing) prior to the date on which the Test is planned to end; and

(b) the final Test Report within 5 Working Days (or such other period as the Parties may agree in writing) of completion of Testing.

8.6 Each Test Report shall provide a full report on the Testing conducted in respect of the relevant Deliverables, including:

(a) an overview of the Testing conducted;

(b) identification of the relevant Test Success Criteria that have been satisfied;

(c) identification of the relevant Test Success Criteria that have not been satisfied together with the Supplier's explanation of why those criteria have not been met;

(d) the Tests that were not completed together with the Supplier's explanation of why those Tests were not completed;

(e) the Test Success Criteria that were satisfied, not satisfied or which were not tested, and any other relevant categories, in each case grouped by Severity Level in accordance with Paragraph 9.1; and

(f) the specification for any hardware and software used throughout Testing and any changes that were applied to that hardware and/or software during Testing.

9 Testing Issues

9.1 Where a Test Report identifies a Test Issue, the Parties shall agree the classification of the Test Issue using the criteria specified in Annex 1 and the Test Issue Management Log maintained by the Supplier shall log Test Issues reflecting the Severity Level allocated to each Test Issue.

9.2 The Supplier shall be responsible for maintaining the Test Issue Management Log and for ensuring that its contents accurately represent the current status of each Test Issue at all relevant times. The Supplier shall make the Test Issue Management Log available to the Authority upon request.

9.3 The Authority shall confirm the classification of any Test Issue unresolved at the end of a Test in consultation with the Supplier. If the Parties are unable to agree the classification of any unresolved Test Issue, the Dispute shall be dealt with

in accordance with the Dispute Resolution Procedure using the Expedited Dispute Timetable.

10 Test Witnessing

10.1 The Authority may, in its sole discretion, require the attendance at any Test of one or more Test Witnesses selected by the Authority, each of whom shall have appropriate skills to fulfil the role of a Test Witness.

10.2 The Supplier shall give the Test Witnesses access to any documentation and Testing environments reasonably necessary and requested by the Test Witnesses to perform their role as a Test Witness in respect of the relevant Tests.

10.3 The Test Witnesses

(a) shall actively review the Test documentation;

(b) will attend and engage in the performance of the Tests on behalf of the Authority so as to enable the Authority to gain an informed view of whether a Test Issue may be closed or whether the relevant element of the Test should be re-Tested;

(c) shall not be involved in the execution of any Test;

(d) shall be required to verify that the Supplier conducted the Tests in accordance with the Test Success Criteria and the relevant Test Plan and Test Specification;

(e) may produce and deliver their own, independent reports on Testing, which may be used by the Authority to assess whether the Tests have been Achieved;

(f) may raise Test Issues on the Test Issue Management Log in respect of any Testing; and

(g) may require the Supplier to demonstrate the modifications made to any defective Deliverable before a Test Issue is closed.

11 Test Quality Audit

11.1 Without prejudice to its rights pursuant to Clause 12.2(b) (Records, Reports, Audits & Open Book Data), the Authority may perform on-going quality audits in

respect of any part of the Testing (each a "Testing Quality Audit") subject to the provisions set out in the agreed Quality Plan.

11.2 The focus of the Testing Quality Audits shall be on:

(a) adherence to an agreed methodology;

(b) adherence to the agreed Testing process;

(c) adherence to the Quality Plan;

(d) review of status and key development issues; and

(e) identification of key risk areas.

11.3 The Supplier shall allow sufficient time in the Test Plan to ensure that adequate responses to a Testing Quality Audit can be provided.

11.4 The Authority will give the Supplier at least 5 Working Days' written notice of the Authority's intention to undertake a Testing Quality Audit and the Supplier may request, following receipt of that notice, that any Testing Quality Audit be delayed by a reasonable time period if in the Supplier's reasonable opinion, the carrying out of a Testing Quality Audit at the time specified by the Authority will materially and adversely impact the Implementation Plan.

11.5 A Testing Quality Audit may involve document reviews, interviews with the Supplier Personnel involved in or monitoring the activities being undertaken pursuant to this Schedule, the Authority witnessing Tests and demonstrations of the Deliverables to the Authority. Any Testing Quality Audit shall be limited in duration to a maximum time to be agreed between the Supplier and the Authority on a case by case basis (such agreement not to be unreasonably withheld or delayed). The Supplier shall provide all reasonable necessary assistance and access to all relevant documentation required by the Authority to enable it to carry out the Testing Quality Audit.

11.6 If the Testing Quality Audit gives the Authority concern in respect of the Testing Procedures or any Test, the Authority shall:

(a) discuss the outcome of the Testing Quality Audit with the Supplier, giving the Supplier the opportunity to provide feedback in relation to specific activities; and

(b) subsequently prepare a written report for the Supplier detailing its concerns,

and the Supplier shall, within a reasonable timeframe, respond in writing to the Authority's report.

11.7 In the event of an inadequate response to the Authority's report from the Supplier, the Authority (acting reasonably) may withhold a Test Certificate (and consequently delay the grant of a Milestone Achievement Certificate) until the

issues in the report have been addressed to the reasonable satisfaction of the Authority.

12 Outcome of Testing

12.1 The Authority shall issue a Test Certificate as soon as reasonably practicable when the Deliverables satisfy the Test Success Criteria in respect of that Test without any Test Issues.

12.2 If the Deliverables (or any relevant part) do not satisfy the Test Success Criteria then the Authority shall notify the Supplier and:

(a) the Authority may issue a Test Certificate conditional upon the remediation of the Test Issues;

(b) where the Parties agree that there is sufficient time prior to the relevant Milestone Date, the Authority may extend the Test Plan by such reasonable period or periods as the Parties may reasonably agree and require the Supplier to rectify the cause of the Test Issue and re-submit the Deliverables (or the relevant part) to Testing; or

(c) where the failure to satisfy the Test Success Criteria results, or is likely to result, in the failure (in whole or in part) by the Supplier to meet a Milestone, then without prejudice to the Authority's other rights and remedies, such failure shall constitute a Notifiable Default for the purposes of Clause 27.1 (Rectification Plan Process).

12.3 The Authority shall be entitled, without prejudice to any other rights and remedies that it has under this Agreement, to recover from the Supplier any reasonable additional costs it may incur as a direct result of further review or re-Testing which is required for the Test Success Criteria for that Deliverable to be satisfied.

13 Issue Of Milestone Achievement Certificate

13.1 The Authority shall issue a Milestone Achievement Certificate in respect of a given Milestone as soon as is reasonably practicable following:

(a) the issuing by the Authority of Test Certificates and/or conditional Test Certificates in respect of all Deliverables related to that Milestone which are due to be Tested; and

(b) performance by the Supplier to the reasonable satisfaction of the Authority of any other tasks identified in the Implementation Plan as associated with

that Milestone (which may include the submission of a Deliverable that is not due to be Tested, such as the production of Documentation).

13.2 The grant of a Milestone Achievement Certificate shall entitle the Supplier to the receipt of a payment in respect of that Milestone in accordance with the provisions of Terms & Conditions Section 6.

13.3 If a Milestone is not Achieved, the Authority shall promptly issue a report to the Supplier setting out:

(a) the applicable Test Issues ; and

(b) any other reasons for the relevant Milestone not being Achieved.

13.4 If there are Test Issues but these do not exceed the Test Issues Threshold, then provided there are no Material Test Issues, the Authority shall issue a Milestone Achievement Certificate.

13.5 Without prejudice to the Authority's other remedies the following shall constitute a Notifiable Default for the purposes of Clause 27.1 (Rectification Plan Process) and the Authority shall refuse to issue a Milestone Achievement Certificate where:

(a) there is one or more Material Test Issue(s); or

(b) the information required under Schedule 8.4 (Reports and Records Provisions) Annex 3 (Virtual Library) has not been uploaded to the Virtual Library in accordance with Paragraph 3 of that Schedule.

13.6 13.6 If there are Test Issues which exceed the Test Issues Threshold but there are no Material Test Issues, the Authority may at its discretion (without waiving any rights in relation to the other options) choose to issue a Milestone Achievement Certificate conditional on the remediation of the Test Issues in accordance with an agreed Rectification Plan provided that:

(a) any Rectification Plan shall be agreed before the issue of a conditional Milestone Achievement Certificate unless the Authority agrees otherwise (in which case the Supplier shall submit a Rectification Plan for approval by the Authority within 10 Working Days of receipt of the Authority's report pursuant to Paragraph 13.3); and

(b) where the Authority issues a conditional Milestone Achievement Certificate, it may (but shall not be obliged to) revise the failed Milestone Date and any subsequent Milestone Date

ANNEX 1: TEST ISSUES – SEVERITY LEVELS

1. **Severity Level 1 Test Issue:** a Test Issue that causes non-recoverable conditions, e.g., it is not possible to continue using a Component, a Component crashes, there is database or file corruption, or data loss;

2. **Severity Level 2 Test Issue**: a Test Issue for which, as reasonably determined by the Authority, there is no practicable workaround available, and which:

   2.1 causes a Component to become unusable;

   2.2 causes a lack of functionality, or unexpected functionality, that has an impact on the current Test; or

   2.3 has an adverse impact on any other Component(s) or any other area of the Services;

3. **Severity Level 3 Test Issue**: a Test Issue which:

   3.1 causes a Component to become unusable;

   3.2 causes a lack of functionality, or unexpected functionality, but which does not impact on the current Test; or

   3.3 has an impact on any other Component(s) or any other area of the Services; but for which, as reasonably determined by the Authority, there is a practicable workaround available;

4. **Severity Level 4 Test Issue:** a Test Issue which causes incorrect functionality of a Component or process, but for which there is a simple, Component based, workaround, and which has no impact on the current Test, or other areas of the Services; and

5. **Severity Level 5 Test Issue:** a Test Issue that causes a minor problem, for which no workaround is required, and which has no impact on the current Test, or other areas of the Services

ANNEX 2: TEST CERTFICATE

To: [NAME OF SUPPLIER]

FROM: [NAME OF AUTHORITY]

[**Date**]

Dear Sirs,

TEST CERTIFICATE

Deliverables: [**insert description of Deliverables**]

We refer to the agreement (the "Agreement") relating to the provision of the Services between the [**name of Authority**] (the "**Authority**") and [**name of Supplier**] (the "**Supplier**") dated [**date**].

Capitalised terms used in this certificate have the meanings given to them in the Terms & Conditions or Schedule 1.4 (Testing Procedures) of the Agreement.

[We confirm that the Deliverables listed above have been tested successfully in accordance with the Test Plan relevant to those Deliverables.]

OR

[This Test Certificate is issued pursuant to Paragraph 12.1 of Schedule 1.4 (Testing Procedures) of the Agreement on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

*delete as appropriate

Yours faithfully

[**Name**]

[**Position**]

acting on behalf of [**name of Authority**]

ANNEX 3: MILESTONE ACHIEVEMENT CERTIFICATE

To: [NAME OF SUPPLIER]

FROM: [NAME OF AUTHORITY]

[Date]

Dear Sirs,

MILESTONE ACHIEVEMENT CERTIFICATE

Milestone: [insert description of Milestone]

We refer to the agreement (the "**Agreement**") relating to the provision of the Services between the [name of Authority] (the "**Authority**") and [name of Supplier] (the "**Supplier**") dated **[date]**.

Capitalised terms used in this certificate have the meanings given to them in the Terms & Conditions or Schedule 1.4 (Testing Procedures) of the Agreement.

[We confirm that all the Deliverables relating to Milestone [number] have been tested successfully in accordance with the Test Plan relevant to this Milestone [or that a conditional Test Certificate has been issued in respect of those Deliverables that have not satisfied the relevant Test Success Criteria.]]*

OR

[This Milestone Achievement Certificate is granted pursuant to Paragraph 13.1 of Schedule 1.4 (Testing Procedures) of the Agreement on the condition that any Test Issues are remedied in accordance with the Rectification Plan attached to this certificate.]*

[You may now issue an invoice in respect of the Milestone Payment associated with this Milestone in accordance with the provisions of Terms & Conditions Section 6)]*

*delete as appropriate

Yours faithfully

[**Name**]

[**Position**]

acting on behalf of [**Authority**]

ANNEX 4: TEST SUCCESS CRITERIA

1 Tests to be Achieved in order to Achieve the ATP Milestone

Test	Pre-Conditions	Test Success Criteria
[List all Tests relating to ATP Milestone]		

2 Tests to be Achieved in order to Achieve a CPP Milestone

CPP Milestone Charge No.	Test	Test Success Criteria
	[List all Tests relating to CPP Milestone Charge No]	

SCHEDULE 2 SERVICE LEVELS AND KPIS

1. Definitions

"Critical Service Level Failure"	shall be the failure to meet a critical Service Level Target for any individual Service Level as specified in the NCTS Service Level Model;
"Major Service Level Failure"	shall be the failure to meet a major failure target for any individual Service Level as specified the NCTS Service Level Model
"Minor Service Level Failure"	shall be the failure to meet a major failure target for any individual Service Level as specified in the NCTS Service Level Model
"Service Credits"	any service credits specified in the NCTS Service Level Model being payable by the Supplier to the Authority in respect of a Service Level Failure;
"Service Credit Cap"	will equal 15% of the monthly charge for the services covered in Schedule 1.1 (Services Description) Sections 3.1 and 3.2;
"Service Level Failure"	means a failure to meet the Service Level Target in respect of a Service Level;
"Service Level Model"	means 'the NCTS Service Level Model
"Service Level Target"	shall be as set out against the relevant Service Level in the NCTS Service Level Model. All Service Level Targets are provided in full in the Service Level Model. For the purpose of the Definitions, Service Level Performance Measure shall be read as Service Level Target;
"Service Hour"	means one hour within the contracted support hours as specified in the Service Level Model;
"Service Day"	means a period during contracted Service Hours e.g., Monday to Friday 07:00 to 19:00
"Service Points"	means the points allocated to each Service Level Target within the NCTS Service Level Model.

2. Service Levels

2.1. If the level of performance of the Supplier:

2.1.1. is likely to or fails to meet any Service Level Target or;

2.1.2. is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify The Authority in writing and the Authority, in its absolute discretion and without limiting any other of its rights, may:

(a) require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Authority and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

(b) instruct the Supplier to comply with the Rectification Plan Process;

(c) if a Service Level Failure has occurred, deduct from the Charges the applicable Service Level Credits payable by the Supplier to the Authority; and/or

(d) if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure in accordance with Terms & Conditions Sections Clause 20 (including the right to terminate for material Default).

2.2. The Supplier shall at all times provide the Services to meet or exceed the Service Level Targets for each Service Level.

2.3. The Supplier acknowledges that any Service Level Failure shall entitle the Authority to the rights set out in Part A of this Schedule 2 including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Authority as a result of the Supplier's failure to meet any Service Level Targets.

2.4. The Supplier shall send Performance Monitoring Reports to the Authority detailing the level of service which was achieved in accordance with the provisions of this Schedule 2.

2.5. A Service Credit shall be the Authority's exclusive financial remedy for a Service Level Failure except where:

2.5.1. the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

2.5.2. the Service Level Failure:

(a) is a Critical Service Level Failure, if relevant; and/or

(e) has arisen due to a Prohibited Act or wilful Default by the Supplier; and/or

(f) results in the corruption or loss of any Government Data; and/or

(g) results in the Authority being required to make a compensation payment to one or more third parties; and/or

2.5.3. the Authority is otherwise entitled to or does terminate this Contract pursuant to the Terms & Condition Clause 20.2;

3. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

3.1. any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

3.2. the Authority shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("**Compensation for Critical Service Level Failure**"),

provided that the operation of this Clause 3 shall be without prejudice to the right of the Authority to terminate this Contract and/or to claim damages from the Supplier for material Default as a result of such Critical Service Level Failure.

Part A: Service Levels and Service Credits

1. Service Levels

1.1 For the purposes of Service Credits, each Service Level is to be assessed independently of other Service Levels.

1.2 For any individual Service Level, a Service Level Failure for any of the Service Level Targets allocated to it will determine the Service Credits due to that Service Level, with materiality of failure determining the Service Points e.g., a major failure in one Service Level Target and a minor failure in a second Service Level Target would determine a Major Service Level Failure for the Service Level.

1.3 Service Levels and performance against Service Level Targets are to be assessed for each Service Period, except where specifically noted otherwise in this Schedule 2.

2. External Factors Affecting Service Levels

1.2 The Supplier shall be entitled to relief from the Service Levels Failures caused by the action or inaction by the Authority or its 3rd Party suppliers who have direct contracts with the Authority provided that the Supplier has notified the Authority promptly and in any event as part of the report in which the relief is claimed. Such relief should relate specifically to the external factor in question and does not void the Service Level for the measurement period.

1.3 The Supplier shall explicitly identify any Service Level Failures that have been excluded either fully or partially from the calculation of performance, and propose where relevant and reasonably possible which third party supplier and/or the Authority action or inaction should be allocated to that Service Level Failure. In the event of a partial exclusion, the Supplier shall also identify the proportion of any Service Points which should accrue to the Supplier as a result of that Service Level Failure.

1.4 For the purposes of calculating Service Credits and Service Points, if the Supplier fails to measure or report on a Service Level in accordance with this Schedule 2 such that the Authority cannot reasonably assess whether the Service Levels have been achieved, it shall be deemed to be Service Level Failure for that Service Level for that Service Period, unless otherwise agreed by the Authority.

2. Service Credits

2.1 The Authority shall use the Performance Monitoring Reports supplied by the Supplier under Part B (Performance Monitoring) of this Schedule 2 (Service Levels and KPIs) to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

2.2 The liability of the Supplier in respect of Service Credits shall be subject to Part A Paragraph 3.4 of this Schedule 2 (Service Levels and KPIs) provided that, for the avoidance of doubt, the operation of the Service Credit Cap shall not affect the continued accrual of Service Credits in excess of such financial limit in accordance with the provisions of this Schedule 2 (Service Levels and KPIs).

2.3 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in Part A of this this Schedule 2 (Service Levels and KPIs).

2.4 the Supplier's aggregate liability in respect of all:

(a) Service Credits; and

(b) Compensation for Critical Service Level Failure;

incurred in any rolling period of 12 months shall be subject to the Service Credit Cap.

3. Repeat Service Level Failures

3.1 In addition to the Service Points incurred via a Service Level Failure for any particular month, repeat failures will incur additional Service Points with an additional 50% of the current month's relevant points for the duration of any failures. Such repeat failure calculations will only apply to an individual Service Level i.e., failures for one Service Level will not cause a repeat failure for other Service Levels.

3.2 For example, for a Service Level with Service Points of 15 (minor) and 20 (major):

Month 1:	Minor Service Level Failure = 15 Service Points
Month 2:	Minor Service Level Failure = 22.5 Service Points (15 + 15/2 x 1 repeat failure month)
Month 3:	Major Service Level Failure = 40 Service Points (20 + 20/2 x 2 repeat failure months)
Month 4:	Minor Service Level Failure = 37.5 Service Points (15 + 15/2 x 3 repeat failure months)
Month 5:	No Service Level Failure for that Service Level = 0 Service Points

4. Amendment of Service Levels and Service Points

4.1 Where a new application or other impacting Change is introduced to this Contract, the Parties shall agree and document new or amendments to the Service Levels which shall apply prior to the release of that Change onto the Live Environment.

4.2 A Service Level is not required to have all three types of Service Level Failure but will always have at least one Service Level Target.

4.3 The Authority may, at its sole discretion, amend the Service Points applicable to the Service Levels to reflect its changing or emergent priorities for the Services.

4.4 For clarity, this includes the allocation of Service Points to Service Levels that previously did not have any Service Points allocated. It may also include the removal of Service Points from that Service Level.

4.5 Following two Major Failures for any individual Service Level within a six-month window, the Authority may instigate a Critical Service Level Failure for that Service Level and therefore define a critical failure target for any/all of the Service Level Targets within the Service Level. Such critical failure targets should be comparable to other comparable services and in line with any other targets already defined for the relevant Service Level.

5. Addition of New or Changed Service Levels

5.1 the Authority may introduce new or changed Service Levels either temporarily (e.g., during the delivery of a Change, or during key business events) or permanently (e.g., in response to changing standards or following a transition of the Services).

5.2 The supplier will adopt the Service Level Model as requested by the Authority. The Authority will provide a reporting template which the supplier will populate from the Authority ITSM tool and other monitoring/analytical tools which the supplier may need to use.

5.3 Such new Service Levels will be implemented through the Change Control Procedure. The Authority will provide a notice period of 30 days of such changes to the Supplier.

Part B: Performance Monitoring

1. Performance Monitoring And Performance Review

1.1 Within twenty (20) Working Days of the Commencement ate the Supplier shall provide the Authority with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

1.2 The Supplier shall provide the Authority with performance monitoring reports (**"Performance Monitoring Reports")** in accordance with the process and timescales agreed pursuant to paragraph 1.1 of Part B of this Schedule 2 (service levels and KPI) which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

1.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

1.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

1.2.3 details of any Critical Service Level Failures;

1.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

1.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

1.2.6 such other details as the Authority may reasonably require from time to time.

1.3 The Parties shall attend meetings to discuss Performance Monitoring Reports (**"Performance Review Meetings"**) on a monthly basis (unless otherwise agreed). The Performance Review Meetings will be the forum for the review by the Supplier and the Authority of the Performance Monitoring Reports. The Performance Review Meetings shall (unless otherwise agreed):

1.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Authority shall reasonably require;

1.3.2 be attended by the Supplier Representative and the Authority Representative; and

1.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Authority Representative and any other recipients agreed at the relevant meeting.

1.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier Representative and the Authority Representative at each meeting.

1.5 The Supplier shall provide to the Authority such documentation as the Authority may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

2. Reporting

2.1 The Supplier will provide monthly reports for the PIs and SLAs set out in the table below. For the avoidance of doubt Service Credits will only apply to SLA.

Measure	KPI/SLA
Incident Management Response	PI
Incident Management Updates	PI

3. Satisfaction Surveys

3.1 The Authority may undertake satisfaction surveys in respect of the Supplier's provision of the Services. The Authority shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Services which the responses to the satisfaction surveys reasonably suggest are not in accordance with this Contract.

Annex 1: Services Levels and Service Credits Table

1. NTCS Standard Service Levels - Incident resolution times

1.1 The intent for the Services is to reasonably minimise the time taken to resolve an incident, based on the priority of incidents. Target and service measures of Service Hours and Service Days are based on contracted supported hours for the Services as per the Service Level Model.

1.2 Incident resolution time to be determined from ServiceNow, being the allocation of the incident through to the point where the ticket is set to resolved. Dataset based on incidents that have been closed during the month.

Priority	Service Level Target: Incident Resolution Time	Service Level Package and Service Hours
P1	4 Service Hours	Standard – 07:00-19:00
P2	8 Service Hours	Standard – 07:00-19:00
P3	1 Standard Service Day	Standard – 07:00-19:00
P4	3 Standard Service Days	Standard – 07:00-19:00
P5	5 Standard Service Days	Standard – 07:00-19:00

Cat	Type of Service Level Failure		Performance Threshold	Failure Severity Levels	Service Points
P1	Minor failure		No more than 1 Fail	>1 fail target	Any Minor failure (and no Major failure): 15 Any Major failure: 20
	Major failure			>2 fail target	
P2	Minor failure		No more than 2 Fail	>2 fail target	
	Major failure			>4 fail target	
P3	Minor failure	>20 incidents	85% of P3 achieve target	>15% fail target	
	Major failure			>20% fail target	
	Minor failure	<20 incidents	No more than 3 P3 Fails	> 3 fail target	
	Major failure			> 4 fail target	
P4	Minor failure	>20 incidents	90% P4 achieve target	>10% fail target	
	Major failure			>15% fail target	
	Minor failure	<20 incidents	No more than 2 P4 Fails	> 2 fail target	
	Major failure			> 3 fail target	
P5	Minor failure	>20 incidents	95% P5 achieve target	>5% fail target	
	Major failure			>10% fail target	
	Minor failure	>20 incidents	No more than 1 P5 Fails	>1 fail target	
	Major failure			>2 fail target	

Where Incident volumes are low (<20) in any given reporting period, a different calculation (which is not based on percentage) is used.

~~Major~~			~~>1~~	~~20~~

2. Service Credit Calculations

2.1 The calculation for Service Credits is calculated using the following:

SC = ((TSP x %) x (SCC)) x AC

SC =	*Service Credit - is the total Service Credit calculated for the relevant Service Period; and payable by the supplier*
TSP =	*Total Service Points - is the total Service Points that have accrued for the relevant Service Period for all KPI failures (Plus any points added for Repeat Failures)*
% =	*is 1%*
SCC =	*Service Credit Cap - is the Service Credit Cap agreed for the contract*
AC =	*Account Charge - is the total Contract Service Charge payable for the relevant Service Period*

SCHEDULE 3 CONTRACT MANAGEMENT PLAN AND MANAGEMENT INFORMATION

1 MANAGEMENT OF THE SERVICES

1.1 Both Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Agreement can be fully realised.

1.2 Both Parties shall pro-actively manage risks attributed to them under the terms of this Agreement and the Supplier shall develop, operate, maintain and (as appropriate) amend processes for the identification and management of risks and issues.

1.3 The Supplier shall provide to the Authority's representatives access to all relevant documentation and/or any part of the Supplier's (or its sub-contractor's) premises as may be reasonably requested by the Authority's representatives, including for the purpose of commercial assurance, risk assessment, security assurance, familiarisation on procedures, audit of the Supplier's compliance with this Agreement and/or site audits. Full details of the Authority's requirement and timescales for the provision of management information reports are set out in Paragraph 3.

1.4 The Authority reserves the right to attend meetings between the Supplier and any subcontractors it utilises to provide the service to ensure proper oversight, management, delivery and performance of the Services and the Suppler shall procure that the Authority has access to such meetings.

1 EFFICIENCY SAVINGS

2.1 As part of routine contract management activities, the Supplier will be required to work with the Authority to realise any possible efficiency savings during the Term. Possible efficiency savings will be reviewed during review meetings pursuant to Paragraph 3 and any savings realised annually will be distributed between the Supplier and the Authority as agreed in advance.

2 REVIEWS

3.1 The Parties shall attend annual performance review meetings, on a date to be agreed between the Parties or, in the absence of such agreement, within 30 Working Days of each anniversary of the Effective Date, to consider the progress of the Agreement, discuss the management information reports and to review any operational issues that have arisen in the preceding review meetings on the following basis.

3.2 The Parties shall agree the format of the review meetings (for example, face to face or telephone conference) in advance.

3.3 The Supplier must provide the Authority with the most up to date management information relating to the period under review at least 5 Working Days before any review meeting.

3.4 Each Party shall procure that those of its contract management team representatives whose attendance is reasonably required to achieve the aims and objectives of the meeting, and any other persons considered by the Authority to be necessary for the review, make all reasonable efforts to attend

review meetings.

3.5 In respect of the period under review, the Authority will take into account any matters it considers necessary, including:

3.5.1 the Supplier's performance in respect of the service levels and KPI's as detailed at Schedule 2 (including any relevant service level trends analysis and whether the service levels reflect improvements in the Services over the Term and any efficiency gains made by the Supplier);

3.5.2 consideration of any changes which may need to be made to the Services; and

3.5.3 a review of future requirements in relation to the Services.

3.6 The Authority shall prepare a report containing its findings from the annual review and discuss with the Supplier how any proposed changes to the Agreement and/or to the Services shall be addressed. Any Contract Changes to be implemented in accordance with this Paragraph shall be implemented in accordance with Schedule 4 (Change Control Procedure).

4 CONTRACT MANAGEMENT ROLES AND DISPUTE ESCALATION POINTS

4.1 The Parties shall assign personnel with the appropriate skills and experience to perform the roles and responsibilities listed in the table below.

Role	Key Personnel	Responsibilities	Contact Name, Title & Contact Details	
			Authority	Supplier
Senior Responsible Owner	No	Overall responsibility for delivery of the Agreement. Level 3 escalation point		
Commercial Director	No	Overall responsibility for the commercial integrity of the Agreement. Level 2 escalation point		
Commercial Lead	No	Responsible for overseeing the contract review process. Level 1 escalation point		

Commercial Manager	Yes	Responsible for monitoring the performance of the Agreement and managing the change control process.		
Contract Manager	Yes	Responsible for the day to day management of the Agreement.		

4.2 Subject to Clause 8.3 and 8.4 (Supplier Personnel and Key Personnel), in the event that the Supplier wishes to replace any of its representatives in the roles listed in Paragraph 4.1, the Supplier shall notify the Authority in writing of the proposed change for the Authority's agreement (such agreement not to be unreasonably withheld or delayed). Notwithstanding the foregoing it is intended that each Authority representative has at all times a counterpart representative of equivalent seniority and expertise.

4.3 The Authority may, by written notice to the Supplier, revoke or amend the authority of any of its representatives in the roles listed in Paragraph 4.1 or appoint a new representative into the role.

5 ADDRESS FOR NOTICES

5.1 The address for notices of the Parties are:

Authority

[redacted]

Supplier

[redacted]

SCHEDULE 4 CHANGE CONTROL PROCEDURE

1 CHANGE CONTROL PROCEDURE

1.1 Either Party may propose a change to this Agreement ("**Contract Change**") in accordance with the procedure for changing the Agreement set out in this Schedule ("**Change Control Procedure**").

1.2 If either Party wishes to propose a Contract Change it shall submit to the other Party a written request substantially in the form set out in Annex 1 detailing the proposed Contract Change ("**Change Request**") specifying, in as much detail as is reasonably practicable, the nature of the proposed Contract Change. As soon as reasonably practicable but in any event within ten (10) Working Days of receipt or issue of a Change Request (as the case may be) the Supplier shall submit to the Authority a written assessment of the Change Request ("**Impact Assessment**").

1.3 Each Impact Assessment shall be completed in good faith and shall include the following information (except where such information is not relevant to the proposed Contract Change):

1.3.1 details of the proposed Contract Change including the reason for the Contract Change;

1.3.2 details of the impact of the proposed Contract Change on the Services and the Supplier's ability to meet its other obligations under this Agreement;

1.3.3 any variations to the terms of this Agreement that will be required as a result of that impact, including proposed changes to the service levels or KPIs or any timetable previously agreed by the Parties;

1.3.4 details of the cost of implementing the proposed Contract Change;

1.3.5 details of the ongoing costs required by the proposed Contract Change when implemented, including any increase or decrease in the Charges, any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;

1.3.6 a timetable and high level plan for the mobilisation of the proposed Contract Change;

1.3.7 details of how the proposed Contract Change will ensure compliance with any applicable Change in Law;

1.3.8 an assessment of the possible risks of introducing the proposed Contract Change; and

1.3.9 such other information as the Authority may reasonably request in (or in response to) the Change Request

1.4 Within fifteen (15) Working Days of receipt of the Impact Assessment, the Authority shall evaluate the Change Request and Impact Assessment and shall notify the Supplier whether it approves or rejects the proposed Contract Change or whether it requires the Supplier to make any changes to the Impact Assessment. If the Authority requires the Supplier to make such changes, the Supplier shall make such modifications within five (5) Working Days of request.

1.5 If the Authority notifies the Supplier that it accepts the proposed Contract Change, then the Supplier shall prepare two (2) copies of a change authorisation note substantially in

the form set out in Annex 2 ("**Change Authorisation Note**") which it shall sign and deliver to the Authority for its signature. Following receipt by the Authority of the Change Authorisation Note, it shall sign both copies and return one copy to the Supplier.

1.6 Until a Change Authorisation Note has been signed and issued by the Authority in accordance with Paragraph 1.5, then:

1.6.1 unless the Authority expressly agrees (or requires) otherwise in writing, the Supplier shall continue to supply the Services in accordance with the existing terms of this Agreement as if the proposed Contract Change did not apply; and

1.6.2 any discussions, negotiations or other communications which may take place between the Authority and the Supplier in connection with any proposed Contract Change shall be without prejudice to each Party's other rights under this Agreement.

2 SUPPLIER'S RIGHT OF REJECTION

2.1 The Supplier shall have the right to reject a Change Request solely in the manner set out in Paragraph 2.2.

2.2 Following an Impact Assessment, if:

2.2.1 the Supplier reasonably believes that any proposed Contract Change which is requested by the Authority would:

(a) materially and adversely affect the risks to the health and safety of any person; and/or

(b) require the Services to be performed in a way that infringes any Law; and/or

2.2.2 the Supplier demonstrates to the Authority's reasonable satisfaction that the proposed Contract Change is technically impossible to implement and neither the Supplier Solution nor the Services Description state that the Supplier does have the technical capacity and flexibility required to implement the proposed Contract Change,

then the Supplier shall be entitled to reject the proposed Contract Change and shall notify the Authority of its reasons for doing so within five (5) Working Days after the date on which it is obliged to deliver the Impact Assessment pursuant to Paragraph 1.2.

3 FAST TRACK CHANGES

3.1 The parties acknowledge to ensure operational efficiency that there may be circumstances where it is desirable to expedite the processes set out above.

3.2 If :

3.2.1 the total number of Contract Changes in relation to which the expedited procedure in this Paragraph 3 ("Fast-track Change Procedure") has been applied does not exceed four (4) in any twelve (12) month period; and

3.2.2 both Parties agree the value of the proposed Contract Change over the remaining Term does not exceed £5,000 and the proposed Contract Change is not significant (as determined by the Authority acting reasonably),

then the parties shall confirm to each other in writing that they shall use the process set out in paragraphs 1 and 2 above but with reduced timescales, such that any period of fifteen (15) Working Days is reduced to five (5) Working Days, any period of ten (10)

Working Days is reduced to two (2) Working Days and any period of five (5) Working Days is reduced to one (1) Working Day.

3.3 The Parties may agree in writing to revise the parameters set out in Paragraph 3.2 from time to time or that the Fast-track Change Procedure shall be used in relation to a particular Contract Change notwithstanding that the total number of Contract Changes to which such procedure is applied will then exceed four (4) in a twelve (12) month period.

4 OPERATIONAL CHANGE PROCEDURE

4.1 Any change in the Supplier's operational procedures which the Parties agree in all respects, when implemented:

4.1.1 will not affect the Charges and will not result in any other costs to the Authority;

4.1.2 may change the way in which the Services are delivered but will not adversely affect the output of the Services or increase the risks in performing or receiving the Services;

4.1.3 will not adversely affect the interfaces or interoperability of the Services with any of the Authority's IT infrastructure; and

4.1.4 will not require a change to this Agreement,

(an "**Operational Change**") shall be processed in accordance with this Paragraph 4.

4.2 Any Operational Changes identified by the Supplier to improve operational efficiency of the Services may be implemented by the Supplier without following the Change Control Procedure for proposed Contract Changes provided they do not:

4.2.1 have an impact on the business of the Authority;

4.2.2 require a change to this Agreement;

4.2.3 have a direct impact on use of the Services; or

4.2.4 involve the Authority in paying any additional Charges or other costs.

4.3 The Authority may request an Operational Change by submitting a written request for Operational Change ("**RFOC**") to the Supplier's contract manager (whose details are set out in Paragraph 4 of Schedule 3).

4.4 The RFOC shall include the following details:

4.4.1 the proposed Operational Change; and

4.4.2 the timescale for completion of the Operational Change.

4.5 The Supplier shall inform the Authority of any impact on the Services that may arise from the proposed Operational Change.

4.6 The Supplier shall complete the Operational Change by the timescale specified for completion of the Operational Change in the RFOC, and shall promptly notify the Authority when the Operational Change is completed.

5 IMPLEMENTATION OF CONTRACT CHANGES

5.1 The Parties shall meet as required and on request by either Party to discuss the order in which agreed Contract Changes are implemented and to monitor the implementation

of such Contract Changes.

6 CHARGES FOR CONTRACT CHANGES

6.1 Each Party will be responsible for any costs they incur as a result of preparing a Change Request or Impact Assessment.

6.2 Both Parties must take all reasonable steps to avoid or minimise additional Charges arising from the implementation of any Contract Change,. If additional resources or costs will be required then the Parties must calculate the cost of the Contract Change in accordance with Schedule 1, Paragraph A5.

7 INDEXATION

7.1 For the avoidance of doubt, The Supplier may not vary Charges to take account of Indexation during the first 3 years of the Term. Where the Term is extended in accordance with Clause 5.2 The Supplier reserves the right to vary the Charges to take account of Indexation once only during the total extension period and only where the UK Consumer Price Indexation (CPI) inflation rate increases by more than 5% as calculated below.

7.2 The adjustment will be calculated by multiplying the relevant amount or sum by the CPI 12-month rate in December of current Contract Year and applied to the Charges in the following Contract year.

7.3 For the purpose of this Clause 7 “Contract Year” shall mean a period of a) 12 months commencing on the Effective Date; or b) thereafter a period of 12 months commencing on each anniversary of the Effective Date.

ANNEX 1: CHANGE REQUEST FORM

CR NO.:	TITLE:	TYPE OF CHANGE (e.g., FAST TRACK):
CONTRACT:		REQUIRED BY DATE:
ACTION:	NAME:	DATE:
RAISED BY:		
AREA(S) IMPACTED (*OPTIONAL FIELD*):		
ASSIGNED FOR IMPACT ASSESSMENT BY:		
ASSIGNED FOR IMPACT ASSESSMENT TO:		
SUPPLIER REFERENCE NO.:		
FULL DESCRIPTION OF REQUESTED CONTRACT CHANGE (INCLUDING PROPOSED CHANGES TO THE WORDING OF THE AGREEMENT):		
DETAILS OF ANY PROPOSED ALTERNATIVE SCENARIOS:		
REASONS FOR AND BENEFITS AND DISADVANTAGES OF REQUESTED CONTRACT CHANGE:		
SIGNATURE OF REQUESTING CHANGE OWNER:		
DATE OF REQUEST:		

ANNEX 2: CHANGE AUTHORISATION NOTE

CR NO.:	TITLE:	DATE RAISED:
CONTRACT:	TYPE OF CHANGE:	REQUIRED BY DATE:
REASON FOR THE CHANGE:		
DETAILED DESCRIPTION OF CONTRACT CHANGE (GIVING FULL DETAILS, INCLUDING ANY SPECIFICATIONS): AND WORDING OF RELATED CHANGES TO THE AGREEMENT:		
COST OF THE CHANGE:		
TIMETABLE:		
IMPACT ON THE AGREEMENT:		

SIGNED ON BEHALF OF THE AUTHORITY:	SIGNED ON BEHALF OF THE SUPPLIER:
Signature:_____	Signature:_____
Name:_____	Name:_____
Position:_____	Position:_____
Date:_____	Date:_____

Schedule 5: Exit Management Plan

1 EXIT MANAGEMENT

1.1 The Supplier shall be required to perform the Services until the end of the Term, including during any notice period given if the Agreement terminates under Clause 20.

1.2 On reasonable notice at any point(s) during the Term, the Supplier shall provide to the Authority such assistance and information as the Authority may reasonably require to assist the Authority and/or its replacement supplier with the orderly transition of the Services from the Supplier to the replacement supplier (or the Authority, as applicable):

1.3 No later than 10 Working Days before the Agreement terminates, the Supplier shall provide the Authority and/or the Replacement Supplier with a complete and uncorrupted version of the Authority Data in electronic form (or such other format as reasonably required by the Authority).

1.4 Upon termination (or earlier if this does not adversely affect the Supplier's performance of the Services and its compliance with the other provisions of this Schedule), the Supplier shall immediately:

1.4.1 cease to use the Authority Data;

1.4.2 erase from any computers, storage devices and storage media that are to be retained by the Supplier after the end of the Term all Authority Data and promptly certify to the Authority that it has completed such deletion. The Supplier shall also delete all copies of any Personal Data unless it is required to be retained by EU or member state laws; and

1.4.3 vacate any Authority premises.

2 EXIT PLAN

2.1 The Supplier shall, within 6 months after the Effective Date, deliver to the Authority an Exit Plan which:

(a) sets out the Supplier's proposed methodology for achieving an orderly transition of the relevant Services from the Supplier to the Authority and/or its Replacement Supplier on the Partial Termination, expiry or termination of this Contract;

(b) complies with the requirements set out in Paragraph 2.2; and

(c) is otherwise reasonably satisfactory to the Authority.

2.2 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 20 Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

2.3 The Parties will work together to review the Exit Management Plan at the start of each contract year.

SCHEDULE 6 SECURITY MANAGEMENT

1 DEFINITIONS

The following definitions apply in this Schedule:

"**Malicious Software**"	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;
"**Software**"	any software which is proprietary to the Supplier or to a third party (or an affiliate83 of the Supplier) or any open source software which, in any case, is or will be used by the Supplier for the purposes of providing the Services.

2 AUTHORITY DATA

2.1 The Supplier shall not delete or remove any proprietary notices contained within or relating to the Authority Data.

2.2 The Supplier shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Supplier of its obligations under this Agreement or as otherwise expressly authorised in writing by the Authority.

2.3 To the extent that Authority Data is held and/or processed by the Supplier, the Supplier shall supply that Authority Data to the Authority as requested by the Authority in the format specified by the Authority.

2.4 The Supplier shall preserve the integrity, confidentiality and accessibility of Authority Data and prevent the unauthorised access, interception, corruption or loss of Authority Data at all times that the relevant Authority Data is under its control or the control of any sub-contractor.

2.5 The Supplier shall perform and maintain secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored off-site in accordance with the security requirements in this Agreement and any business continuity and disaster recovery plan. The Supplier shall ensure that such back-ups are available to the Authority (or to such other person as the Authority may direct) at no additional cost to the Authority, and that the data contained in the back-ups are available at all times upon request and are delivered to the Authority at no less than six (6) monthly intervals (or such other intervals as may be agreed in writing between the Parties).

2.6 The Supplier shall ensure that any system on which the Supplier holds any Authority Data, including back-up data, is a secure system that complies with the security requirements in this Agreement.

2.7 If the Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's

Default so as to be unusable, the Authority may:

2.7.1 require the Supplier (at the Supplier's expense) to restore or procure the restoration of Authority Data to the extent and in accordance with the requirements specified in any business continuity and disaster capability plan and the Supplier shall do so as soon as practicable but not later than five (5) Working Days from the date of receipt of the Authority's notice; and/or

2.7.2 itself restore or procure the restoration of Authority Data, and shall be repaid by the Supplier any reasonable expenses incurred in doing so to the extent and in accordance with the requirements specified in any business continuity and disaster capability plan.

2.8 If at any time the Supplier 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 Supplier shall notify the Authority immediately and inform the Authority of the remedial action the Supplier proposes to take.

3 SECURITY REQUIREMENTS

3.1 The Supplier shall comply with the security management plan set out at Annex 1 ("**Security Management Plan**") and the security policy identified as such within the Security Management Plan ("**Security Policy**").

3.2 The Authority shall notify the Supplier of any changes or proposed changes to the Security Policy.

3.3 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the Services it may submit a Change Request (as defined in Schedule 4). In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall then be agreed in accordance with the Change Control Procedure in Schedule 4.

3.4 Until and/or unless a change to the Charges is agreed by the Authority pursuant to the Change Control Procedure in Schedule 4 the Supplier shall continue to perform the Services in accordance with its existing obligations.

4 MALICIOUS SOFTWARE

4.1 The Supplier shall, as an enduring obligation throughout the Term, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.

4.2 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.

4.3 Any cost arising out of the actions of the Parties taken in compliance with the provisions of Paragraph 4.2 shall be borne by the Parties as follows:

4.3.1 by the Supplier where the Malicious Software originates from the Software or the Authority Data (whilst the Authority Data was under the control of the Supplier)

unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Authority when provided to the Supplier; and

4.3.2 otherwise by the Authority.

ANNEX 1: SECURITY MANAGEMENT PLAN

Security Plan Questionnaire (High)

To:	**Netcompany UK Limited**
From:	**HMRC**
Date:	**28/01/2022**
Tender reference:	**N/A**
Tender title:	**NCTS**

Schedule 2.4 Security Plan

Background
The Contractor is required to prepare a Security Plan in accordance with the HMRC's Security Policy. The requirements set out in this Security Plan also apply to any sub-contractors engaged by the Contractor to perform any of the services under the Contract. HMRC has developed a standard set of questions and recommendations (see attached Appendices) to ensure consistency across relevant contracts. The Contractor is required to provide answers to the standard set of questions contained within this questionnaire to formulate the initial Security Plan. This Security Questionnaire covers the principles of protective security to be applied in delivering the services in accordance with HMRC's Security Policy and Standards The Contractor's response to this questionnaire, with any subsequent amendments as may be agreed as part of a clarification process, will be included in the signed version of any resulting agreement, as confirmation that the content of the Security Plan has been agreed with HMRC.

1	Policy & Standards	Supplier Response

1a	Please confirm that you understand that your responses to this questionnaire will form the initial Security Plan and will be included in the final signed version of any resulting agreement.	**Confirmation of understanding of the responsibilities based on the responses and that this will form the initial Security Plan.**
1b	Please confirm your organisation and any subcontractors' will conform to the requirements set out in the Government Security Policy Framework (SPF), available from Security Policy Framework and any Security Requirements recorded in the schedules and/or Order Form.	**Netcompany UK Limited and any subcontractor will conform to the requirements set out in the Government Security Policy Framework (SPF) and any Security Requirements recorded in the schedules and/or Order Form.**
1c	If you believe that the Public Sector Network (PSN) Code of Connection, available from www.gov.uk, will apply to your organisation and any sub-contractors, please provide details of how you will conform to this.	**PSN requirements related to technical interoperability documents and obligations for network services as well as Code of Interconnection (CoICo) seem to be relevant. Contractor-related network architecture, testing and reporting will be included.**
1d	Please confirm that your organisation and any sub-contractors will handle HMRC assets in accordance with legislation including the UK General Data Protection Regulation see UK GDPR and in accordance with Clause 23 (*Protection of Personal Data*) of the Contract.	**Confirm that Netcompany UK Limited and any sub-contractors will handle HMRC assets in accordance with legislation including the UK General Data Protection Regulation see UK GDPR and in accordance with Clause 23 (Protection of Personal Data) of the Contract.**

1e	Please confirm that you have paid the Data Protection Fee to the ICO or that you fall into one of the exempt categories. More information can be found here	**Data Protection Fee to the ICO has been paid. The following information is available as reference.** **Registration number:** ZA066989 **Date registered:** 22 July 2014 **Registration expires:** 21 July 2023 **Payment tier:** Tier 3 **Data controller:** Netcompany UK Limited **Address:** 1st Floor, Northburgh House 10 Northburgh Street London, EC1V 0AT United Kingdom

1f	Please provide details of any security accreditation that your organisation currently possesses, such as but non-exclusive to, ISO 27001 and PCI DSS and describe the process used to achieve the accreditation.	**Netcompany UK Limited is certified with:** **1. ISO 27001:2018** **4.ISO 14001:2015** **2. ISO 20000-1:2018** **3. ISO 9001:2015**
1g	If you intend to involve sub-contractors at any stage during the Contract please list them and provide details of how you will ensure their compliance with all aspects of this Security Plan.	
1h	As appended to this Schedule 2.4, Appendix G, Security Aspects Record, defines the Government Security Classifications (see Government Security Classifications) carried by the HMRC data. If you are successful in the tender process, you will require a Security Manager (or appointed person), to take responsibility for the security of the data. Please provide the name of your Security Manager who will act as a first point of contact and conduct ongoing management of security risks and incidents (including identification, managing, and reporting in line with agreed procedures for actual or suspected security breaches).	**Project-focused Security Manager will be designated**
2	**Physical Security** (For requirements please see Appendix A – Physical Security)	**Supplier Response**

2a	For the locations where HMRC assets are held please provide details of any procedures and security in place designed to control access to the site perimeter. Detail measures such as fencing, CCTV, guarding, and procedures and controls in place to handle staff and visitors requesting access to the site. Please also provide details of the maintenance schedule of your security controls.	**Physical Access Controls:** - **Fencing** - **CCTV 24x7** - **Interior & Exterior Guarding 24x7** - **Badges & Escorting** - **Secure Access Control Areas (Building entrance)** **Security technical controls are under at least annual maintenance**

2b	Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas within the premises holding HMRC assets. Detail measures such as building construction type, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls. Please also include details of any automated access controls, alarms and CCTV coverage. Please also provide details of the maintenance schedule of these security controls.	**Regarding the building that will host HMRC assets:** 1. **Building construction type: ??** 2. **Availability of lockable storage: Yes with combination of access card & Biometrics** 3. **Procedures covering end of day/silent hours** 4. **Procedures for visitors: visitor's escorting and visitor's badge** 5. **Alarms in place** 6. **CCTV coverage in place** 7. **Key management: ??** **Security technical controls are under at least annual maintenance.**
3	**IT Security** (For requirements please see Appendix B – IT Security)	
3a	Please state what, if any, form of assessment in relation to the Government backed Cyber Essentials Scheme has been performed or provide details of any cyber essentials accreditation that you are planning in the future.	**ISO 27001 based internal audits** **ISO 27001 annual review** **OWASP ASVS requirements verification**
3b	Please provide details of the controls and processes you have in place covering patching, malware (anti-virus), boundary/network security (intruder detection), content checking/blocking (filters), lockdown (prevention), and how regularly you update them.	**Process in place:** 1. **Patching** 2. **Malware (antivirus) & EDR Security** 3. **Boundary/Network Security(IDS),** 4. **Content filtering checking/blocking** 5. **IPS** **The regular update is scheduled every**

3c	Please provide details of the overall security and access control policy of your systems covering physical and electronic assets (including communications connection equipment, e.g., bridge, routers, patch panels). You should record details of the formal registration/deregistration process, how users are Authorised, Authenticated and held Accountable for their actions. Also include details of the measures in place to manage privilege access e.g., System Administrators and remote users.	**1. CICO procedures in place** **2. AD Authentication + 2FA** **3. Personalised accounts** **4. Use of VPN – FortiClient solution for authorization of remote users and Administrators**
3d	Please provide details of how your security and access control policy complies with the Security Policy Framework (including where necessary, use and control of backup systems, network storage and segregation of HMRC data (including 'cloud' solutions), and additional security for more sensitive information assets).	**1. Back-up and restore procedures are in place and they are regularly executed** **2. HMRC data are separated to a dedicated virtual storage where they are network segregated.**
3e	Please describe how you ensure all software and data is approved before being installed, and how your information systems are reviewed for compliance with security implementation standards (e.g., penetration testing).	**1. Testing procedure is followed in order to ensure software and data installation.** **2. Application Penetration Testing is being executed before the go live period.** **3. Infrastructure Vulnerability Assessment is regularly executed (at least annually)**
3f	Please provide details of the controls and processes (including level of encryption and controlled access procedures) you have in place for the use of portable media and storage devices exceptionally loaded with HMRC data.	**Bitlocker in place for disk encryption** **External media can also be blocked for any project team members**

3g	Please provide details of how all equipment (e.g., hardware, portable media) that holds or has held data will be destroyed or decommissioned, and how all data will be rendered unreadable and irretrievable in line with HMG Security Policy Framework requirements for information management.	**NETCOMPANY UK LIMITED upon request or/and upon project termination will follow the established "Disposal of Media" procedure which dictates the appropriate methods of data sanitization in accordance with the classification level of information the media contains.**
4	**Personnel Security** (For requirements please see Appendix C – Personnel Security)	
4a	What security vetting has been carried out for staff who will have access to, or come in to contact with HMRC data or assets.	**Background check** **Non-disclosure agreement signed**
4b	Please provide details of how you will ensure that all staff accessing HMRC data are aware of the confidential nature of the data and comply with their legal and specific obligations under the Contract.	**All Netcompany UK Limited staff participates in regular InfoSec Awareness trainings where access and handling of confidential information is analysed.** **Additionally, there is a Corporate DLP solution in place.**
4c	All contractor's personnel who have access to HMRC data, and/or are directly involved in the service provision must sign a copy of HMRC's Confidentiality Agreement. Please confirm that, in the event that your bid is successful, you will provide signed hard copies of the CA for all personnel involved in this Contract if requested.	**All the Netcompany UK Limited personnel and subcontractors have signed Non-Disclosure agreement.**
4d	Please provide details of the ongoing training you provide to staff in respect of data security, including risk awareness and the identification and reporting of security incidents. Please also provide details of your documented information security procedures and processes that are available to all staff who will have access to, or come into contact with HMRC data.	**Regular (at least annual) information security awareness trainings including the following areas:** - **Secure data access and handling** - **Information Security Incident – Recognition and Reporting** - **Corporate Information Security Classification Procedure and Schema** **There are documented policies, procedures and processes as part of the Corporate Information Security Framework (certified by ISO27001)**

4e	Please provide details of your procedures for on and off boarding staff	**Check in – Check Out (CICO) procedures are followed for on boarding and off boarding staff.**
5	**Process Security** (For requirements please see Appendix D – Process Security)	
5a	Please provide details of the format in which HMRC data will be held, how you will ensure segregation of HMRC data, and the locations where this data will be processed.	**TBC**
5b	Please confirm your understanding and agreement that the transfer of any HMRC asset to third parties (any individual or group other than the main Contractor) is prohibited without prior written consent from HMRC. If you anticipate transferring data, especially using portable media during the delivery of this project, please set out your proposed transfer procedures for consideration.	**Confirmed that there is full understanding and agreement that the transfer of any HMRC asset to third parties (any individual or group other than the main Contractor) is prohibited without prior written consent from HMRC**.

5c	Please confirm that you understand that HMRC Data must not be processed or stored outside the United Kingdom without the express permission of HMRC. If you are considering transferring data outside of the UK, please provide details on how and where the data will be processed or stored. To the extent that any data offshoring would include the transfer of Personal Data (as defined in the United Kingdom General Data Protection Regulation (UK GDPR)) outside of the UK, please provide details of the protections and safeguards which would be applied to ensure that such data is afforded a level of protection that is essentially equivalent to that guaranteed in the UK by UK GDPR, including in relation to access to the data by the country's public authorities. Please note: In line with HMRC's current policies, the successful supplier(s) will not be permitted to transfer any Personal Data provided by HMRC in connection with any contract resulting from this procurement exercise to any country outside of the UK where such transferred data will not be afforded a level of protection essentially equivalent to that guaranteed in the UK by UK GDPR. On this basis, HMRC reserves the right to reject a bidder's entire tender submission and/or terminate any contract awarded where it becomes apparent to HMRC that the supplier is	**Confirmed that Netcompany UK Limited understands that HMRC Data must not be processed or stored outside the United Kingdom without the express permission of HMRC.**

	transferring/is proposing to transfer Personal Data outside of the UK without ensuring the transferred data is afforded a level of protection essentially equivalent to that guaranteed in the UK by UK GDPR.	
5d	In order to protect against loss, destruction, damage, alteration or disclosure of HMRC data, and to ensure it is not stored, copied or generated except as necessary and authorised, please provide details of the technical and organisational measures you have in place (including segregation of duties and areas of responsibility) to protect against accident or malicious intent.	• **DLP solution in place.** • **Separation of duties (SoD) in place at every corporate department regarding user level and access.**
5e	What arrangements are in place for secure disposal of HMRC assets that may be in your possession once no longer required?	**NETCOMPANY UK LIMITED upon request or/and upon project termination will follow the established "Disposal Of Media" procedure which dictates the appropriate methods of data sanitization in accordance with the classification level of information the media contains.**
5f	How and when will you advise HMRC of security incidents that impact HMRC assets that may be in your possession?	**The advice of HMRC for security incidents will be through PM or/and Information Security Officer.**
5g	Please describe your disciplinary procedures in the event of a security breach involving HMRC data.	**There will be a dedicated security officer/manager for the project. There is a dedicated corporate Security Information Response Team (SIRT) in case of a security breach.**
5h	Do you have a List X accreditation? If 'yes', please answer the following: • What is the name of your Security Controller? • What/Where does the List X accreditation cover? • For what purpose? • Please provide evidence the Department who sponsored the List X accreditation has agreed to share the environment.	• **N/A**

6	**Business Continuity**	
6a	Please provide an overview of your organisation's Business Continuity and disaster recovery plans in terms of the HMRC data under the Contract, or attach a copy of your Business Continuity Plan. Please specify if you operate Business Continuity or disaster recovery from outside the UK. Also, please provide details on when and how frequently these plans are tested and advise when they were last tested and confirm results of testing exercises are available for review if requested. Please provide details on how you will meet recovery times if these have been specified in the schedules and/or Order Form.	**NETCOMPANY UK LIMITED has and maintains a business continuity plan and business continuity testing procedures, which include but are not limited to the areas of disaster recovery planning and pandemic planning. NETCOMPANY UK LIMITED reviews, updates, and tests the business continuity plan annually and, can provide a summary of the business continuity plan and test results upon request. NETCOMPANY UK LIMITED Business Continuity and Disaster Recovery activities and tooling are operated within the EU area.**
7	**Cryptography**	
7a	Please provide details of processes and procedures in place for handling Government cryptographic material.	**Cryptographic controls are in place such as:** **1. DB encryption** **2. Use of Bitlocker for endpoint encryption** **3. Encrypted connections (Over TLS / IPSec)** **4. Transport Security Layer (TLS 1.3) for REST APIs** **5. Key Management** **6. Signed & Encrypted Messaging Communication (Email)**

The following appendices provide additional information on the types of security control that <u>may</u> be expected as a minimum for the protection of HMRC information, data and assets.
It is not a legally binding document, nor does it provide a definitive list of baseline security controls. It should be read in conjunction with HMG and HMRC Security Policy and Standards.

Appendix A – Physical Security

Please consider: the effect of topographic features and landscaping on perimeter security; the possibility of being overlooked; the ease of access and communications; the existence and proximity of public rights of way and neighbouring buildings; the existence of emergency and evacuation routes from adjacent buildings; the implications of shared accommodation; the location of police and emergency services; the build of the structure.

Building Security - There should be as few points of exit and entry as possible but in line with Health & Safety and Fire Regulations. Where exit and entry points exist then physical security controls, such as window bars, grilles shutters Security Doors etc may be installed. The effectiveness of these protection measures may be enhanced by the use of Intruder Detection Systems (IDS), CCTV or Guard Service.

Physical Security	Requirements	Recommended
Secure Rooms	Construction in line with CPNI guidance; locked during 'silent hours' and keys/combinations secured. Sufficient CPNI-Approved lockable storage for material at OFFICIAL or above. Intruder alarm with key holder response.	Intruder alarm with police response. Appropriate automated access control system.
Perimeter Security		CCTV Coverage to identify intruders with adequate lighting for night-time operation. Use of fencing that offers a degree of resistance to climbing and to deter an opportunist e.g., anti-intruder fencing. Manned guarding to be considered.
Physical Access - secure areas	Visitors limited to those with a business need, issued with identifying badges upon arrival and escorted at all times.	A visitor log maintained and visitors sign in and out.

Physical Security	Requirements	Recommended
Building	Constructed of robust building materials typically, brick or lightweight block walls. External doors of solid construction, locked during silent hours and linked to intruder detection system. Access to keys must be checked and any lock combinations changed at regular intervals not exceeding 12 months. A record of key/combination holders must be maintained. The number of keys to a lock must be kept to a minimum. Spare keys must not be held in the same container as 'working keys'. The premises must be locked during 'silent hours' and keys secured. Intruder alarm with key holder response. Windows double glazed or similar unit with locks. Emergency exit doors included on intruder detection system.	Security Keys should not be removed from the premises. Intruder alarm with police response. Power outage alarm with key holder response. Appropriate automated access control system.
Environmental	Fire risk assessment must be carried out. Uninterruptible power supply for security and health & safety equipment.	Smoke detection system e.g., VESDA.
Transport and Storage	Appropriate CPNI-Approved lockable storage for HMRC material. Point to point transfer of all HMRC material using CPNI-Approved locked containers and (where necessary) solid sided vehicles.	HMRC "trusted hand" using named individuals.

Appendix B – IT Security

IT Security	Requirements	Recommended
Cyber Essentials	It is **mandatory** for HMG suppliers to demonstrate that they meet the technical requirements prescribed by Cyber Essentials.	Cyber Essentials Plus with independent assessment and certification.

IT Security	Requirements	Recommended
Authorisation	Users and Administrators must be authorised to use the System/Service. Higher privilege access accounts should be tightly controlled and only assigned to authorised individuals.	
Authentication[1]	Individual passwords must be used to maintain accountability; Robust passwords should be used, that are designed to resist machine based attacks as well as more basic guessing attacks. Passwords must be stored in an encrypted form using a one-way hashing algorithm. Passwords must be able to be changed by the end user, if there is suspicion of compromise. Passwords must be changed at least every 3 months.	Machine-generated passwords. Multi-factor authentication should be considered for exposed environments and remote access. Passwords for privileged accounts/users (Administrators) etc. should be changed more frequently than every 3 months.
Access Control	User access rights to HMRC information assets must be revoked on termination of employment. Audit logs for access management in place showing a minimum of 30 days of activity.	

[1] Authentication is the process by which people "prove" to the system that they are the person they claim to be. There are three possible authentication factors: Passwords (something a person knows), tokens (something a person possesses), and biometrics (something a person inherently is or how they behave).

IT Security	Requirements	Recommended
Malware Protection[2]	Malware protection software should be installed on all computers connected or able to connect to the Internet. It must be regularly updated in line with vendor recommendations or at least daily and should be configured to scan files on access and perform regular scans of all files at server and desktop level (PC/Laptop etc). It should also be configured to identify and block access to known malicious websites. Security Operating Procedures (SyOps) must ensure that malware protection is kept up to date. Anti-Virus Administrators and users should be trained on use of AV software. Users should receive awareness training so that they are aware of risks posed by malicious code from the use of email and attachments, internet and removable media (CD, DVD, USB devices etc). All users, systems and services must be provided on a least privilege basis to reduce the potential for accidental introduction of malicious code. For systems attaching to HMRC network, dual layered malware protection and detection capability.	Consideration should be given to allowing privilege users (System Administrators) to only use a limited 'non-privilege role' to conduct vulnerable operations such as browsing or importing via removable media. Dual layered malware protection and detection capability. Malware protection software should be configured to update automatically or update through the use of a centrally managed deployment. Systems and services holding assets with a Government Security Classification of Secret are expected to be air-gapped and will therefore require malware protection to be configured manually.

[2] CESG Good Practice Guide No 7 provides information on the threats and vulnerabilities and risks associated with malicious code and also provides guidance on appropriate risk management measures.

IT Security	Requirements	Recommended
Network Security	Information, applications and computers within the organisation's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices. Boundary controls should have content checking and a blocking policy in place e.g., firewalls. As a minimum the default administrative password for network devices such as Firewalls should be changed to a strong password comprising of a minimum of 8 characters. All unnecessary services should be disabled/'blocked' by default at the boundary firewall. It is important that Firewall rules that are no longer required are disabled/removed timeously, for example when a service is no longer required. The administrative interface used to manage boundary firewall configuration routinely must NOT be accessible from the Internet.[3]	Dual paired firewalls, different vendors. Anomaly detection capability e.g., Network intruder detection system.
Patch Management	Software should be patched and devices, systems, operating systems and applications should be 'locked down' to remove unnecessary services and functionality. File types should be limited. All Critical security patches should be deployed timeously and in line with vendor recommendations. The deployment of Important i.e., less critical patches should be deployed on the basis of risk.	
System Documentation	System designs/architectural blue prints and network designs should be protected from unauthorised access, loss and destruction.	
Disposal of media	HMRC information assets must be sanitised in line with HMG IA Infosec Standard 5 Secure Sanitisation. Your CESG contact can provide further information.	

[3] It is envisaged that systems holding Secret assets will not be supported by a remote administrative and will not be Internet facing.

IT Security	Requirements	Recommended
Technical Testing	IT health check aka penetration testing for front facing internet services delivered to HMRC.	Consideration for regular IT health check of application and infrastructure services delivered to HMRC.
Use of Laptops and removable recordable media.	Laptops holding any information supplied or generated as a consequence of a Contract with HMRC must have, as a minimum, a FIPS 140-2 approved full disk encryption solution installed. Approval from HMRC must be obtained before information assets are placed on removable media[4]. This approval must be documented sufficiently to establish an audit trail of responsibility. All removable media containing information assets must be encrypted. The level of encryption to be applied is determined by the highest HM Government Security Classification of an individual record on the removable media. Unencrypted media containing HMRC information assets must not be taken outside secure locations; the use of unencrypted media to store HMRC information assets must be approved by HMRC.	

Appendix C – Personnel Security

Personnel Security	Requirements	Recommended
Security Clearance	Pre-employment checks should meet the Baseline Personnel Security Standard (BPSS) and must be completed for all staff with potential or actual access to HMRC assets. Security Clearance for all staff with access or potential access to material with a Government Security Classification of SECRET.	See www.gov.uk specifically the link to the Disclosure & Barring Service for more information. Staff with privileged system access (system administrators) to have Developed Vetting Clearance.
Confidentiality Agreements	Confidentiality Agreements (CA) must be completed by all staff with potential or actual access to HMRC information assets as requested.	

[4] The term drives includes all removable, recordable media e.g., memory sticks, compact flash, recordable optical media and external hard drives.

Personnel Security	Requirements	Recommended
Security Awareness Training	All staff must undergo security awareness training and be familiar with HMRC security policy, standards and guidance. There must be a plan in place, endorsed and owned by a named individual at Board Level, to ensure refresher training takes place at least annually.	Board members and senior management should be able to demonstrate their commitment to security through a variety of mechanisms.
Joiners and leavers	Process to ensure individuals are appointed to clearly defined roles with appropriate access rights only. Leavers' access rights to systems and premises are removed on termination of employment.	

Appendix D – Process Security

Process Security	Requirements	Recommended
Disciplinary Process	There must be an organisational disciplinary process. Staff must be briefed on this and the penalties that may result from failure to comply with documented security policies	
Security Policies, Processes and Procedures	Where the contract requires you to hold HMRC assets at Secret or above you MUST ensure there is a relationship at senior management level between your organisation and CESG. Procedures in place to determine whether any compromise of HMRC assets e.g., loss or modification of information, software and hardware has occurred. Procedures for the handling and storage of HMRC information assets must be established to protect from unauthorised disclosure and/or misuse. End of day procedures must ensure that HMRC assets are adequately protected from unauthorised access. A clear desk policy must be enforced. Procedures must be in place to ensure HMRC's assets are segregated from any other Client's assets held by the contractor. Procedures for the secure disposal of the HMRC's assets must be in place.	Obtain the services of a CLAS consultant to help you through the bidding process and, if successful, the early stages of contract award.

Process Security	Requirements	Recommended
	Where HMRC assets are held at SECRET all staff and visitors must visibly wear an identifying pass while on site. Where HMRC assets are held at SECRET portable media devices must be excluded from the secure area. A challenge culture must be fostered, so that staff or visitors not wearing a pass are challenged. Where an access control system is in operation tailgating must be discouraged. Where required HMRC assets must be destroyed in line with the Security Policy Framework. Further guidance on storage and destruction of media is available from CESG.	
Transfer of HMRC Data	Any proposed transfer of HMRC data must be approved by HMRC in writing. If the Contractor is unsure whether approval has been given, the data transfer must not proceed. Where data transfers are necessary in the performance of the Contract, they should be made by automated electronic secure transmission via the Government Secure Internet (GSI) with the appropriate level of security control. Individual data records (unless as part of a bulk transfer of an anonymised respondent survey data) will require specific transfer arrangements. Transfer of aggregated data such as results, presentations, draft and final reports may also need discussion and agreement, again in advance of any such transfer.	**Whenever possible, putting data on to removable media should be avoided.** Where this is unavoidable, hard drives and personal digital assistants, CD-ROM/DVD/floppy/USB sticks are only to be used after discussion and agreement with HMRC in advance of any such transfer. If the use of removable media is approved, data must be written to them in a secure, centralised environment and be encrypted to HMRC's standards. If you anticipate transferring data on removable media during the delivery of this project please set out your proposed transfer procedures.
Incident Management	Arrangements must be in place for reporting security breaches to the asset owner.	
List X	Further information on List X is available at www.gov.uk. A List X accreditation may just cover a floor, a room or even a particular piece of secure furniture and may be for a specific purpose.	

Process Security	Requirements	Recommended
	Note: If you do have a List X accreditation, please keep responses generalised for the purposes of completion of this question.	

Appendix E – Business Continuity

Business Continuity Requirements	Requirements	Recommended
Business Continuity Management	3rd party suppliers should provide HMRC with clear evidence of the effectiveness of its Business Continuity management arrangements and alignment with recognised industry standards, by assessing risks to their operations and producing and maintaining business continuity documentation.	

Appendix F – Cryptography

Government Cryptography	Requirements	Recommended
Cryptographic Material	Information on this subject will be available from your contact in CESG.	

Schedule 2.4 – Appendix G – Security Aspects Record

G.1. This contract will involve the Contractor holding UK Government security classified material (*replace "security classified" with "classified" for overseas companies*). It is a condition of this contract that this material must be protected. The standard of protection required is detailed below and varies with the level of security classification. Material passed to the Contractor will bear the security classification appropriate to it.

G.2 In determining the Security Classification 'Aggregated Material' has been considered. 'Aggregation' is the term used to describe the situation when a large number of data items at one classification are collected together. The impact of the compromise of the whole collection can often be significantly higher than the Impact of compromise of one item. This applies to compromises of Confidentiality, Integrity and Availability.

G. 3 To assist the Contractor in allocating any necessary classification to material which the Contractor may produce during the course of the contract and thus enable the Contractor to provide the appropriate degree of protection to it, this schedule formally advises you of the correct security classification to apply to the various aspects of the contract.

G.4 The highest security classification of the information with which the Contractor operates under this contract is *[Insert classification here]*.

G.5. The aspects of the contract which require a Security Classification are:-

Aspect	Security Classification
(provide full and detailed information)	

G.6. If the contract contains a Condition of Clause referring to "Secret Matter" this Secret matter is defined as the Aspects listed above.

G.7. The Contractor is responsible for ensuring that the level of protective marking associated with the various aspects listed above have been brought to the attention of the person directly responsible for the security of this contract, that they are fully

understood, and that the required security controls in the contract security conditions can and will be taken to safeguard the material concerned.

G.8 At the outset of this contract the person identified by the Contractor who will take responsibility for the security of the classified material:

Name: Role:

G.9 If during the term of the contract the person responsible for the security of the classified material changes, then the Contractor must advise the Client at the earliest opportunity.

SCHEDULE 7 DATA PROTECTION

1 DATA PROTECTION

The following definitions apply in this Schedule:

"Data Protection Legislation"	(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; (iiii) 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;
"Controller", "Processor", "Data Subject", "Personal Data Breach", "Data Protection Officer"	take the meaning given in the GDPR;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Processor 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"	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"	Data Protection Act 2018;
"LED"	Law Enforcement Directive (Directive (EU) 2016/680);
"Protective Measures"	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 Clause 16 (Authority Data and Security Requirements and Schedule 1 (Services Description);

"Sub-processor"	any third Party appointed to process Personal Data on behalf of that Processor related to this Agreement.

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor. The only processing that the Processor is authorised to do is listed in Annex 1 by the Controller and may not be determined by the Processor.

1.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

1.3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

1.3.1 a systematic description of the envisaged processing operations and the purpose of the processing;

1.3.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

1.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

1.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

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

1.4.1 process that Personal Data only in accordance with Annex 1, unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by Law;

1.4.2 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:

(a) nature of the data to be protected;

(b) harm that might result from a Data Loss Event;

(c) state of technological development; and

(d) cost of implementing any measures;

1.4.3 ensure that:

(a) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Annex 1);

(b) 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:

(i) are aware of and comply with the Processor's duties under this Paragraph 1;

(ii) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

(iii) 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

(iv) have undergone adequate training in the use, care, protection and handling of Personal Data; and

1.4.4 not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(a) 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;

(b) the Data Subject has enforceable rights and effective legal remedies;

(c) 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

(d) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;

1.4.5 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.

1.5 Subject to Paragraph 1.6, the Processor shall notify the Controller immediately if it:

1.5.1 receives a Data Subject Request (or purported Data Subject Request);

1.5.2 receives a request to rectify, block or erase any Personal Data;

1.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

1.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

1.5.5 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

1.5.6 becomes aware of a Data Loss Event.

1.6 The Processor's obligation to notify under Paragraph 1.5 shall include the provision of further information to the Controller in phases, as details become available.

1.7 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 Paragraph 1.5 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

1.7.1 the Controller with full details and copies of the complaint, communication or request;

1.7.2 such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

1.7.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

1.7.4 assistance as requested by the Controller following any Data Loss Event;

1.7.5 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.

1.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Paragraph 1. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

1.8.1 the Controller determines that the processing is not occasional;

1.8.2 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; or

1.8.3 the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Processor shall allow for audits of its Data Processing activity related to the scope of this Agreement by the Controller or the Controller's designated auditor, not more frequently than once per year and upon at least 10 Working Days prior written notice.

1.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.

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

1.11.1 notify the Controller in writing of the intended Sub-processor and processing;

1.11.2 obtain the written consent of the Controller;

1.11.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this Paragraph 1 such that they apply to the Sub-processor; and

1.11.4 provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

1.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

1.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this Paragraph 1 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

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

ANNEX 1 PROCESSING, PERSONAL DATA AND DATA SUBJECTS

Personal data processed under this contract is hypothetical test data and will not be used in Live environments. Therefore, completion of this Schedule is N/A.

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

The contact details of the Controller's Data Protection Officer are: [redacted]

The contact details of the Processor's Data Protection Officer are:
Contact Person: [redacted]
e-mail : [redacted]

The Processor shall comply with any further written instructions with respect to processing by the Controller.

Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	*[This should be a high level, short description of what the processing is about i.e., its subject matter of the contract.* *Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public.]*
Duration of the processing	*[Clearly set out the duration of the processing including dates]*
Nature and purposes of the processing	*[Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by*

	automated means) etc. *The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*
Type of Personal Data being Processed	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*
Categories of Data Subject	*[Examples include: staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]*
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	*[Describe how long the data will be retained for, how it be returned or destroyed]*