£

# G-Cloud 14 Call-Off Contract

This Call-Off Contract for the G-Cloud 14 Framework Agreement (RM1557.14) includes:

## G-Cloud 14 Call-Off Contract

Part A: Order Form 2

Part B: Terms and conditions 11

Schedule 1: Services 32

Schedule 2: Call-Off Contract charges 33

Schedule 3: Collaboration agreement 34

Schedule 4: Alternative clause 47

Schedule 5: Guarantee 51

Schedule 6: Glossary and interpretations 60

Schedule 7: UK GDPR Information 77

Annex 1: Processing Personal Data 77

Annex 2: Joint Controller Agreement 80

Schedule 8: Corporate Resolution Planning 87

Schedule 9 : Variation Form 104

## Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier’s prepopulated version unless it has been carefully checked against template drafting.

|  |  |
| --- | --- |
| **Platform service ID number** | 652307018506035 |
| **Call-Off Contract reference** | SR2368360228 |
| **Call-Off Contract title** | Online Trade Tariff |
| **Call-Off Contract description** | The UK Integrated Tariff Tool is a digital platform, hosted by the Supplier in AWS cloud. The tool helps Traders determine duties, licences, and restrictions for the products they are importing and exporting including facilitations/obligations introduced by the Windsor Framework Agreement. Traders use the tool for guidance by identifying the necessary commodity code to complete import/export declarations and other paperwork. This helps determine the correct amount Customs Duty and import VAT payable. The Supplier will provide ongoing maintenance and support of this existing tool, and also manage and implement future improvements and enhancements to this tool in future.  |
| **Start date** | 1 April 2025 |
| **Expiry date** | 31 March 2028 |
| **Call-Off Contract value** | £10,900,000 |
| **Charging method** | Fixed Price Outcomes/Deliverable, Capped Time and Materials, or Time and Materials at the Buyers sole discretion |
| **Purchase order number** | Buyer will provide  |

This Order Form is issued under the G-Cloud 14 Framework Agreement (RM1557.14).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Services offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

|  |  |
| --- | --- |
| **From the Buyer** | HM Revenue and Customs 100 Parliament StreetLondon SW1A 2BQ |
| **To the Supplier** | Transform UK Consulting Ltd (part of Next 15)Telephone: 0203 128 800060 Great Portland StreetLondonW1W 7RTUnited KingdomCompany number: 01579589 |
| **Together the ‘Parties’** |

###  Principal contact details

### Call-Off Contract term

|  |  |
| --- | --- |
| **Start date** | This Call-Off Contract Starts on **1 April 2025** and is valid for 36 months. |
| **Ending****(termination)** | The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6).The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1). |
| **Extension period** | This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. |

### Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

|  |  |
| --- | --- |
| **G-Cloud Lot** | This Call-Off Contract is for the provision of Services Under:* Lot 3: Cloud support
 |
| **Additional Services** | Any additional services in relation to the Online Trade Tariff Services will be requested in writing by the Buyer |
| **Location** | The Services will be delivered to HM Revenue and Customs at various addresses. |
| **Quality Standards** | The quality standards required for this Call-Off Contract are detailed within Schedule 1. |
| **Technical Standards:** | The technical standards required for this Call-Off Contract are detailed within Schedule 1. |
| **Service level agreement:** | The service level and availability criteria required for this Call-Off Contract are detailed within Schedule 1. |
| **Onboarding** | Not Applicable. |

|  |  |
| --- | --- |
| **Offboarding** | The offboarding plan for this Call-Off Contract will be developed and agreed between the Buyer and Supplier within three (3) months of the Start Date. The plan may include an exit plan with processes, costs, responsibilities, etc. |
| **Collaboration agreement** | Not Applicable. |
| **Limit on Parties’ liability** | The annual total liability of either Party for all Property Defaults will not exceed £10m, capped at £1m for each individual claim.The annual total liability for Buyer Data Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).The annual total liability for all other Defaults will not exceed the greater of 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). |
| **Buyer’s responsibilities** | The Buyer is responsible for: * Ensuring that the Supplier has access to any HMRC services required to develop and deploy a working service and any other services identified and communicated and agreed with the Buyer.
* Providing access to HMRC premises if/when required.
* Notifying the Supplier of any changes or proposed changes to the Security Policy
 |
| **Buyer’s equipment** | The Buyer’s equipment to be used with this Call-Off Contract includes:* SDES
 |

### Supplier’s information

|  |  |
| --- | --- |
| **Subcontractors or partners** | Transform is not planning to use subcontractors for this work.  |

### Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

|  |  |
| --- | --- |
| **Payment method** | The payment method for this Call-Off Contract is BACS. |
| **Payment profile** | The payment profile for this Call-Off Contract is monthly in arrears. |
| **Invoice details** | The Supplier will issue electronic invoices monthlyin arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice. |
| **Who and where to send invoices to** | The payment method for this Call-Off Contract is by BACS transfer through the HMRC Ariba network |
| **Invoice information required** | All invoices must include:• the Purchase Order number. • total value excluding Value Added Tax (VAT). • the VAT percentage. • the total value including VAT.• a contact name and telephone number of an appropriate individual in the Supplier's finance department in the event of administrative queries; and• the banking details for payment to the Supplier via electronic transfer of funds (name and address of bank, sort code, account name and number).In addition to the invoice, an accompanying change-log Excel spreadsheet must also be issued to the operational and commercial contract managers, The changelog will provide details of all changes which have been actioned, including the following information: • a change reference number • the Buyers name of who raised the change• a brief description of the change • the resource impact and • monthly invoice reference number |
| **Invoice frequency** | Invoice will be sent to the Buyer monthly. |
| **Call-Off Contract value** | The total value of this Call-Off Contract is £10,900,000 |

### Additional Buyer terms

|  |  |
| --- | --- |
| **Performance of the** **Service** | Not applicable. |
| **Guarantee** | Not applicable. |
| **Warranties, representations** | Not applicable. |
| **Supplemental requirements in addition to the Call-Off** **terms** | The Supplier shall comply with the security management plan set out at Schedule 1 (11) (“Security Management Plan”) and the security policy identified as such within the Security Management Plan (“Security Policy”). The Supplier shall comply with the Authority’s mandatory terms as set out in Schedule 1 (12) of this Call-Off Contract. For the avoidance of doubt and contrary to any other provision relating to precedence of terms in this Call-Off Contract, in case of any ambiguity or conflict, the Authority’s mandatory terms in Schedule 1 will supersede any other terms in this Call-Off Contract. |
| **Alternative clauses** | Not Applicable. |
| **Buyer specific****amendments****to/refinements of the Call-Off Contract terms** | Not Applicable. |
| **Personal Data and** **Data Subjects** | Confirm whether Annex 1 (and Annex 2, if applicable) ofSchedule 7 is being used: [**Delete as appropriate**] Annex 1, Annex 2 |
| **Intellectual Property** | No Project Specific IPR. |
| **Supplier Social Value commitment** | We will engage with relevant stakeholders to understand existing framework activities and how we can deliver additional environmental benefits through our service provision. Our team has started an Open-Source project – Zekia – a Cloud Carbon (cloud agnostic) tracking tool for our development team and are in discussions with Defra and Government Digital Services to expand the use and contributors to this project. Green Engineering – Part of our Carbon Reduction plan is a framework assessing the impact of Carbon emissions and embedding this into the development lifecycle. We will share this with CCS and discuss how to include it in our delivery. Planet Centred Design - Our Service Design practice are collaborating with partners and clients to create a community of interest around Planet Centred Design practices and we’d welcome the opportunity to involve CCS in this initiative. Digital footprint – Our new website - deployed 1st February 2024 – is currently 88% cleaner than all web pages globally. We will continue to measure its sustainability using 3 different calculators. We have worked with clients like BEIS and Borderforce to reduce their digital footprint. We aim to co-design/co-create relevant environmental training to influence CCS’ chosen staff, suppliers and communities. We run Environmental Sustainability training for staff, suppliers and clients through our internal academy (Learnamp), e.g. ISO awareness training, Environmental Management System training and BCorp familiarisation. Events - We run multiple events for our staff, clients and key stakeholders: Series of talks by inspirational speakers (e.g. Paddy Loughman), about climate change and the ecological crisis and the pathways we can take through it; Partnering with Plantega to run tasting sessions focusing on making plant-based eating super convenient. We are subscribers to Gartner to keep ahead of eco-technology. We are members of techUK and participate in their Sustainability Strategy Forum. |
| **Performance Indicators** | Data supplied by the Supplier in relation to Performance Indicators is deemed the Intellectual Property of the Buyer and may be published by the Buyer. |

###

### 1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clauses 8.3 to 8.6 inclusive of the Framework Agreement.

### 2. Background to the agreement

2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.14.

|  |  |  |
| --- | --- | --- |
| **Signed** | Supplier | Buyer |
| **Name** |  |  |
| **Title** |  |  |
| **Signature** |  |  |
| **Date** |  |  |

2.2 The Buyer provided an Order Form for Services to the Supplier.

## Part B: Terms and conditions

###

### 1. Call-Off Contract Start date and length

 1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 36 months

### 2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses, schedules and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

* 2.3 (Warranties and representations)
* 4.1 to 4.6 (Liability)
* 4.10 to 4.11 (IR35)
* 5.4 to 5.6 (Change of control)
* 5.7 (Fraud)
* 5.8 (Notice of fraud)
* 7 (Transparency and Audit)
* 8.3 to 8.6 (Order of precedence)
* 11 (Relationship)
* 14 (Entire agreement)
* 15 (Law and jurisdiction)
* 16 (Legislative change)
* 17 (Bribery and corruption)
* 18 (Freedom of Information Act)
* 19 (Promoting tax compliance)
* 20 (Official Secrets Act)
* 21 (Transfer and subcontracting)
* 23 (Complaints handling and resolution)
* 24 (Conflicts of interest and ethical walls)
* 25 (Publicity and branding)
* 26 (Equality and diversity)
* 28 (Data protection)
* 30 (Insurance)
* 31 (Severability)
* 32 and 33 (Managing disputes and Mediation)
* 34 (Confidentiality)
* 35 (Waiver and cumulative remedies)
* 36 (Corporate Social Responsibility)
* paragraphs 1 to 10 of the Framework Agreement Schedule 3

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the ‘Framework Agreement’ will be a reference to the ‘Call-Off Contract’

2.2.2 a reference to ‘CCS’ or to ‘CCS and/or the Buyer’ will be a reference to ‘the Buyer’

2.2.3 a reference to the ‘Parties’ and a ‘Party’ will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause ‘XX’, where ‘XX’ is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

### 3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier’s Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer’s acceptance criteria, as defined in the Order Form

### 4. Supplier staff

4.1 The Supplier Staff must:

 4.1.1 be appropriately experienced, qualified and trained to supply the Services

 4.1.2 apply all due skill, care and diligence in faithfully performing those duties

 4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

 4.1.4 respond to any enquiries about the Services as soon as reasonably possibl 4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier’s engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14 digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

### 5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

 5.1.3 have raised all due diligence questions before signing the Call-Off Contract

 5.1.4 have entered into the Call-Off Contract relying on their own due diligence

### 6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.

6.2 The Supplier’s business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer’s own plans.

### 7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier’s delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer’s failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there’s an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn’t possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer’s volumes indicated in the Order Form are indicative only.

### 8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

### 9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

 9.4.2 receipts for the insurance premium

 9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

###

### 10. Confidentiality

10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

###

### 11. Intellectual Property Rights

11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights (“IPR”s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trademarks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer’s or its relevant licensor’s Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 The Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer’s written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier’s or its relevant licensor’s IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;

(b) alleging that the Buyer Data violates, infringes or misappropriate any rights of a third party;

(c) arising from the Supplier’s use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgement against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer’s obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier’s breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party’s IPRs because of the:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier’s performance of the Services

11.6.3 use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.7.1 modify the relevant part of the Services without reducing its functionality or performance

11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

11.8.1 the use of data supplied by the Buyer which the Supplier isn’t required to verify under this Call-Off Contract

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

### 12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer’s written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer’s instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

### 13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier’s and Buyer’s security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework:

https://www.gov.uk/government/publications/security-policy-framework and the Government Security - Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.npsa.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets: https://www.npsa.gov.uk/sensitive-information-assets

13.6.3 the National Cyber Security Centre’s (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: https://www.gov.uk/government/publications/technologycode-of-practice/technology -code-of-practice

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:

https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6.6 Buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer’s Data.

### 14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technologycode-of-practice/technology -code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN’s security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

### 15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

### 16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer’s written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer’s security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

16.4.1 Supplier’s expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

16.4.2 Buyer’s expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer’s control

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer’s Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer’s Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government’s ‘10 Steps to Cyber Security’ guidance:

https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

###

### 17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

### 18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days’ written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier’s obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer’s right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier’s avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn’t pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn’t relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

###

### 19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

* 7 (Payment, VAT and Call-Off Contract charges)
* 8 (Recovery of sums due and right of set-off)
* 9 (Insurance)
* 10 (Confidentiality)
* 11 (Intellectual property rights)
* 12 (Protection of information)
* 13 (Buyer data)
* 19 (Consequences of suspension, ending and expiry)
* 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability),

24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 Any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer’s written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

* 1. Each Party will return all of the other Party’s Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.
	2. All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

###

### 20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

* Manner of delivery: email
* Deemed time of delivery: 9am on the first Working Day after sending
* Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

### 21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier’s own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier’s methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer’s own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer’s right to take the Term beyond 36 months is subject to the Buyer’s own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from CDDO under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier’s additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier’s Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

###

### 22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier’s possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

### 23. Force majeure

23.1 Neither Party will be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Contract (other than a payment of money) to the extent that such delay or failure is a result of a Force Majeure event.

23.2 A Party will promptly (on becoming aware of the same) notify the other Party of a Force Majeure event or potential Force Majeure event which could affect its ability to perform its obligations under this Call-Off Contract.

23.3 Each Party will use all reasonable endeavours to continue to perform its obligations under the Call-Off Contract and to mitigate the effects of Force Majeure. If a Force Majeure event prevents a Party from performing its obligations under the Call-Off Contract for more than 30 consecutive Working Days, the other Party can End the Call-Off Contract with immediate effect by notice in writing.

###

### 24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer’s liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier’s liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

### 25. Premises

25.1 If either Party uses the other Party’s premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer’s premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer’s premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer’s premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

### 26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

### 27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who is not a Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

### 28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

### 29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to end it, and within 28 days of the Buyer’s request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

 29.2.1 the activities they perform

 29.2.2 age

 29.2.3 start date

 29.2.4 place of work

 29.2.5 notice period

 29.2.6 redundancy payment entitlement

 29.2.7 salary, benefits and pension entitlements

 29.2.8 employment status

 29.2.9 identity of employer

 29.2.10 working arrangements

29.2.11 outstanding liabilities

 29.2.12 sickness absence

 29.2.13 copies of all relevant employment contracts and related documents

29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer.

29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.5 The Supplier will cooperate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.6.1 its failure to comply with the provisions of this clause

29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

* 1. The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
	2. For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

### 30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn’t have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

### 31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer’s contractors

31.2.2 co-operate and share information with the Buyer’s contractors to enable the efficient operation of the Buyer’s ICT services and G-Cloud Services

### 32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract using the template in Schedule 9 if it isn’t a material change to the Framework Agreement or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request using the template in Schedule 9. This includes any changes in the Supplier’s supply chain.

32.3 If either Party can’t agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days’ notice to the Supplier.

###

### 33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are

 reproduced in this Call-Off Contract document at Schedule 7.

## Schedule 1: Services

**HMRC Online Trade Tariff Tool – Services**

### **1. Overview**

1.1. The UK Integrated Tariff encompasses all duties, licences and restrictions for imports and exports. Traders will use this tool for guidance when importing/ exporting goods including facilitations/obligations introduced by the Windsor Framework Agreement. Once traders have identified the necessary commodity code they need within the tool, it will help to complete import/export declarations and other paperwork and will display the correct amount Customs Duty and import VAT payable (subject to information provided by trader).

1.2. The tool will also help traders to check if a licence or certificate is required to move the goods (e.g., products of animal origin, specific medicines, or chemicals).

1.3. Over 1 million unique external users access the Online Trade Tariff per annum.

### **2. General Requirements**

###

2.1 The Supplier will have:

Current understanding and knowledge of Trade Tariff,

Experience working with both UK and NI Tariffs,

Current understanding and knowledge of the Windsor Framework

Experience working with and producing AI driven solutions

Expertise in trade policy,

An understanding of cross Government departmental systems such as CHIEF & Customs Declaration Service (CDS), and

Baseline Personal Security Standard (BPSS) clearance for all personnel as sociated with the delivery of the required Service.

2.2. The supplier will maintain compliance with ISO 27001 (for quality and technical standards).

2.3. The supplier will adhere to a clearly defined and agreed commissioning process, outlining any new work to be undertaken.

2.4. The supplier will issue electronic invoices monthly in arrears.

2.5 The supplier will notify HMRC if support hours consumed are above the monthly profile set out in the contract.

**3. The Services**

3.1. The Supplier to provide ongoing maintenance and support of the Online Trade Tariff Tool to ensure its successful operation and to maintain availability as set out in the Service Level Agreement, including the following (list is not exhaustive):

3.1.1. Communication with HMRC, Government Digital Service (GDS), maintenance, and continued development of UK Online Trade Tariff tool, on the suppliers AWS platform.

3.1.2. Supply of specialist cloud services for the maintenance and development for the Online Trade Tariff tool.

3.1.3. To work with the Buyer to ensure availability of Online Trade Tariff following changes to data feed, resulting from the implementation of the new CDS.

3.1.4. Carry out user research, propose recommended changes and execute the changes approved by the Buyer.

3.1.5. Provide analysis of customer feedback, assisting HMRC to identify trends, flaws, and enhancements. Including feedback on CDS and the ED Tariff product.

3.1.6. Import the Tariff Application Platform file (National data) to the Online Trade Tariff database as required by the buyer, providing support to Buyer’s CDS/DIT teams if necessary.

3.1.7. Liaise with CDS & DIT colleagues if errors/ inconsistencies are identified and provide support to rectify where necessary.

3.1.8. Support CDS trade testing as required by the Buyer.

3.1.9. Map the customer journey, the process, and create user research stories.

3.1.10. Contribute towards the improvement of the Online Trade Tariff tool search functionality.

3.1.11. Provide Trade Tariff analytics access to the Buyer.

3.1.12. Provide access to the Supplier’s digital, analytic dashboard.

3.1.13. Support and develop 3rd party APIs to access OTT database.

3.1.14. Support and develop Windsor Framework specific 3rd party APIs.

3.1.15. Support and develop AI driven tools, models and APIs.

3.1.16 Complete customer journey mapping/ Process mapping/ User research and story creation

3.1.17. Develop OTT to introduce user accounts and AI driven search tools

3.1.18. Improve trade Tariff search functionality.

3.1.19. Provide Trade Tariff analytics access to Buyer. Provide access to digital, analytic dashboard.

3.1.20. Maintain improvements log and proactively review with Buyer: search synonyms improvements, A-Z duplications and corrections, EU description typos, chapter notes improvements.

3.2. The Supplier to manage and implement changes, improvements, and enhancements to the Online Trade Tariff Tool which will be requested by:

3.2.1. The Buyer completing a request for services to define the requirement,

3.2.2. The Supplier to respond with a proposal and formal quotation (including a breakdown of the proposed costs), and

3.2.3. Signature approval from both Parties to formalise.

3.3. A template request for service can be found at Annex 1, below.

**4. Continuous Improvements**

4.1. The Supplier will maintain an improvements log, and proactively review with the Buyer the following: a) Buyer printing, b) Search synonyms improvements, c) A-Z duplications and corrections, d) EU description typos, and e) Chapter notes improvements, such as hyperlinks instead of references to other goods.

**5. Security and Disaster Recovery**

The Supplier will:

5.1. Deploy security patches and upgrades to vulnerabilities within a maximum period from the public release of such patches within a maximum period of fourteen (14) days except where the Buyer agrees a different period after a case-by-case consultation with the Supplier.

5.2. Detect, analyse, and respond to service outages in accordance with the Service Level Agreement. Collaborating with the Buyer and the GDS team.

5.3. Perform incident management and reporting relating to outages and security up grades in accordance with the Service Level Agreement.

5.4. Apply fixes identified as part of incident management to prevent service degradation and to detect, analyse, and respond to service outages.

5.5. Undertake penetration testing at least once a year, or if a significant change to the infrastructure takes place.

5.6. Use the latest versions of anti-virus definitions and software from an industry-accepted software vendor to provide protections against and minimise the impact of cyber-attacks.

5.7. Monitor service interactions within the solution platform, ensuring they are traceable and monitored end to end.

5.8. Provide, and seek Buyer’s approval of, their Business Continuity Plan in support of the Service and review and update at least once every 12 months.

5.9. In the event of a security breach, the Supplier will inform HMRC within a maximum of 24 hours of detection of such anomalous or unauthorised activity within their premises or environment and take all reasonable measures to remediate the position.

5.10. Work with the Buyer to identify potential impacts and interdependencies arising from changes with the Buyers other Customs system to the Online Trade Tariff tool and related service(s). Implement consequential changes as agreed with the Buyer.

**6. Upgrades**

6.1. The Supplier will ensure any routine maintenance takes place outside of standard operating hours (07:00-19:00 on weekdays (Monday to Friday), excluding public holidays) and must be non-disruptive.

**7. Support**

The Supplier will:

7.1. Attend Monthly performance review meetings (face-to-face or virtually, via video-call (e.g., via Microsoft Teams). The format of these meetings is to be arranged and agreed between Buyer and Supplier, as and when they are scheduled).

7.2. Provide monthly incident reports – which include a breakdown of:

7.2.1.1. Performance against KPIs as defined in the below Service Level Agreement, and

7.2.1.2. Service incidents which have occurred and/or are ongoing within that monthly reporting period.

7.3. Maintain collaborative and open communication with HMRC, Government Digital Service (GDS) and Government PaaS team, to ensure the maintenance and continued development of the Online Trade Tariff tool on Government PaaS platform on Cloud Foundry.

7.4. Standard support will be provided between the hours of 09:00 and 17:00 on week days (Monday to Friday), excluding public holidays. By exception and by prior agreement from the Buyer, work will take place on weekends or national holidays subject to formal agreement with the Engine project lead and the client.

7.5. Monitor a shared mailbox inbox in order to support the service hours as stated in 7.4 above, between those hours. The address is hmrc-trade-tariff-support-g@digital.hmrc.gov.uk

7.6. Provide technical support, maintenance, and continued development of the service domain, including the preparation and submission for appropriate live service assessments.

7.7. Provide the Service and ensure its availability and functionality the Services Level Agreement and Key Performance Indicators.

### **8. Service Level Agreement (“SLA”)**

**8.1.** The 4-tier urgency / impact matrix below can be used to ascertain the priority level of support incidents in relation to this Contract. This is defined in Table 1, below.

*Table 1 – Urgency/Impact Matrix*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Priority**  |  | **Impact**  |  |  |
| 1 (High)  | 2  | 3 (Low)  |
| **Urgency**  | 1 (High)  | Priority 1 – Critical  | Priority 2 - High  | Priority 3 - Medium  |
| 2  | Priority 2 - High  | Priority 3 - Medium  | Priority 4 - Low  |
| 3  | Priority 3 - Medium  | Priority 3 - Medium  | Priority 4 - Low  |
| 4 (Low)  | Priority 4 - Low  | Priority 4 - Low  | Priority 5 – Very Low  |

**8.2.** The urgency and impact levels will be determined according to these criteria:

*Table 2 – Priority Levels*

|  |  |  |
| --- | --- | --- |
| **Priority Level**  | **Impact**  | **Target resolution**  |
| **P1 - Critical**  | * Major Business Impact, with > 50% users unable to access a national service or incorrect output is likely to mislead the public.
* The damage caused by the Incident increases rapidly.
* Activities that cannot be completed are highly time sensitive.
* A minor Incident can be prevented from becoming a major Incident by acting immediately.
 | 4 working hours  |
| **P2 – High**  | * Significant Business Impact 10% - 50% users unable to access a national service or business critical function unavailable or working incorrectly.
* The damage caused by the Incident increases considerably over time.
 | 8 working hours  |
| **P3 - Medium**  | * Significant Business Impact < 10%
* Specific users unable to access elements of service or non-business critical function unavailable or working incorrectly.
 | 3 working days  |
| **P4 – Low**  | * No Immediate Business Impact.
* Problem with a record which disrupts or prevents normal processing.
 | 7 working days  |
| **P5 – Very low**  |  Nuisance issue that does not impact the ability of users to complete the required tasks  | 28 working days  |

### **9. Key Performance Indicators (“KPIs”)**

**9.1.** KPI 1: Availability

*Table 3 – KPI #1*

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Indicator**  | **Service Level Performance Criteria**  | **Service Level** **Performance** **Measure**  | **Service Credit for each Service Period**  |
| **Availability**  | The Supplier will provide Service Availability of 99.00% within the Supported Time using the following measure:   ST – PD – UD \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ x 100 ST – PD  Where: ST (Supported Time) = the hours that the Online Trade Tariff Tool is available, being 07:00-19:00 Monday-Friday (excl. bank holidays)  PD (Planned Downtime) = periods of downtime agreed in advance with the Buyer, not to exceed 7 hours and 20 minutes per month, including weekends  UD (Unplanned Downtime) = any downtime which is not Planned Downtime   | **99.00%**  | 2% Service Credit of the monthly invoice charge (excluding VAT), for **minor** service level failure.  5% Service Credit of the monthly invoice charge (excluding VAT), for **major** service level failure.  *Refer to Table 4 for definition of minor and major service level failure*  |

*Table 4 – Service Level Failure Definitions*

|  |  |
| --- | --- |
|  | **Failure Severity Level**  |
| **Performance Threshold**  |  **Minor Major**  |
| **<99.00%, but >98.00% availability achieved in the reporting period**  | **<98.00%, availability achieved in the reporting period**  |

9.1.1. By exception, matters outside of the Supplier’s control, such as planned maintenance on behalf of the hosting service provider (gov.uk PaaS) will not be counted within this metric, but will be reported on by the Supplier in a monthly feedback package.

This feedback package will be provided on a monthly basis, and include documentary evidence of the following, which may then be discussed at the quarterly performance review meeting with HMRC:

* Evidence of uptime backed up by metrics from service's reporting systems (New Relic).
* Summary of CDS data loads including any issues discovered.
* Summary of feedback received from members of the public during the previous month period.
* Documentation of any support updates that have been made during the prior month.

**9.2.** KPI 2: Quality

*Table 5 – KPI #2*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Key** **Indicator**  | **Service Level Performance** **Criteria**  | **Service Level** **Performance** **Measure**  | **Performance Threshold**  | **Service Credit for each Service Period**  |
| **Quality**  | Upon receipt from the Buyer, the Supplier will deliver data updates to the Online Tariff in accordance with the programme schedule.  | **24 hours**  | **48 hours**  | 1% Service Credit of the monthly invoice charge (excluding VAT) where the Performance Threshold is exceeded  |

9.2.1. The Supplier will commit to delivering data updates within 24 hours to the Online Tariff according to the enhanced current schedule, which will be shared with the Supplier, upon Contract Award.

### **10. Training**

**10.1.** The Supplier will ensure that all appropriate training is delivered at the Buyer’s request, to ensure the Buyer’s personnel can use the service effectively.

11. **Security Management 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.
 |
| **For Information** |
| * 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.
* 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 terms of the contract*.*
* 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.
* HMRC Data must not be offshored without the express permission of HMRC. ‘Offshoring’ means transferring the data outside of the UK, including by **storing it or accessing it** outside of the UK.
 |

|  |
| --- |
| **1 Policy & Standards** |
| 1. 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](https://protect.checkpoint.com/v2/r06/___https%3A//ico.org.uk/ktw-twlfsnxfyntsxdifyf-uwtyjhynts-kjjdxjqk-fxxjxxrjsyd___.ZXV3MjpuZXh0MTU6YzpvOjZhMTZkNGQyNDAwZjA1YmMwNmZiODE0ZDE4MDE0NWRjOjc6ZWM3NDoyMTI0NDJkMzJkZWU3ODZkNzUwNGM1YmE5Mzg5OWY5N2RkNzE4ZmIxOTEzODI2ZDhlZjg2MzhlZGU4OWI2YzM2OnA6VDpU)
 |
| **Confirmed.** |
| 1. Please provide details of any security accreditation that your organisation currently possesses, such as but not exclusive to, ISO27001 and PCI DSS.
 |
| **ISO9001, ISO27001, Cyber Essentials, Cyber Essentials Plus** |
| 1. If you intend to involve sub-contractors at any stage during the Contract please list them, the function/service they will provide and provide details of how you will ensure their compliance with all aspects of this Security Plan.
 |
| **No sub-contractors.** |
| 1. 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).
 |
| **Robert Sugrue - Group Head of Information & Cyber Security – Next 15 Group** |
| **2 Physical Security** (For requirements please see Appendix A – Physical Security) |
| 1. 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.
 |
| **Transform, 60 Great Portland Street, London W1W 7RT:*** **Next 15 offices are closed workspaces and are occupied solely by Next 15 Group companies.**
* **Access control mechanisms such as key cards and numeric keypads are fitted to all ingress/egress points and secure internal locations.**
* **Area’s housing sensitive information or systems for the storage, transfer, or processing of data are restricted to ensure only authorised employees are permitted access.**
* **CCTV systems exist in Transform offices including at all ingress and egress points; these retain video recordings for at least 30 days.**
* **Visitors to Transform facilities must show valid identification, have an employee sponsor their visit, sign a visitor log, and wear a visitor identification badge.**
 |
| 1. 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.
 |
| **Transform, 60 Great Portland Street, London W1W 7RT:*** **Next 15 offices are closed workspaces and are occupied solely by Next 15 Group companies.**
* **Access control mechanisms such as key cards and numeric keypads are fitted to all ingress/egress points and secure internal locations.**
* **Area’s housing sensitive information or systems for the storage, transfer, or processing of data are restricted to ensure only authorised employees are permitted access.**
* **CCTV systems exist in Transform offices including at all ingress and egress points; these retain video recordings for at least 30 days.**
* **Visitors to Transform facilities must show valid identification, have an employee sponsor their visit, sign a visitor log, and wear a visitor identification badge.**
 |
| **3 IT Security** (For requirements please see Appendix B – IT Security)  |
| 1. Please provide details of the controls and processes you have in place for the following, and how regularly you update them.
 |
| * Patching – **Patching across on all systems is undertaken on a regular basis**
 |
| * Malware (anti-virus) – **Centrally managed anti-virus and malware solution implemented on all devices**
 |
| * Boundary/network security (intruder detection) – **Centrally managed and in place**
 |
| * Content checking/blocking (filters) – **Centrally managed email and URL filtering in place**
 |
| * Lockdown (prevention) – **Centrally managed EDR/SIEM/SOC allows lock of machines, accounts and file locations**
 |
|  |
| 1. Please provide details of the overall security and access control policy of your systems covering physical and electronic assets. 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.
 |
| * **Security Assertion Markup Language through a common identity provider has been implemented on Transform systems wherever feasible to enable centralized access and session control and to provide single sign-on capabilities.**
* **Multifactor authentication with a minimum of two factors is required for all Transform user accounts.**
* **Password policy is compliant with the most current guidelines from the UK NCSC and NIST standard publication 800-53b.**
* **Policy requires at least 12 characters and a combination of uppercase, lowercase, special characters, and numbers for all passwords.**
* **Accounts are locked after consecutive invalid attempts.**
* **A password policy enforcement tool is used to extend the default policy set in Microsoft Active Directory to include the following additional criteria:**
	+ **No common dictionary words, no character patterns, no passwords that include parts of the username, no previously breached passwords**
* **Passwords are securely communicated and must be changed upon first logon.**
* **System passwords are changed from their default passwords.**
* **A user’s identity must be validated prior to the IT team performing a password reset.**
* **System administrators adhere to the tenet of least privilege and separation of duties; each are assigned with a standard and privileged account; both accounts are delegated minimum rights necessary for administrative and non-administrative job functions.**
* **Duties are segregated to prevent opportunities for collusion.**
* **For non-system administrators, role-based access controls are used following the least privilege principle to ensure access is only permitted on a need-to-know basis.**
* **User accounts are reviewed by their IT suppliers Next 15; this includes a review of inactive accounts, third-party (vendor /supplier) accounts, privileged accounts, service accounts, and authentication methods.**
* **Access is terminated immediately following the reception of an employee termination notification**
 |
| 1. 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).
 |
| **As above.** |
| 1. 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).
 |
| **Vendor risk management in place to assess all new suppliers and software. Continuing program of both internal and external penetration testing.** |
| 1. 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. (Including laptops and mobile phones)
 |
| **We do not use portable storage media / drives. The use of BYOD (personal mobiles) is restricted to email and controlled.** |
| 1. 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.
 |
| **End of life equipment and media is disposed of by third-party providers who certify destruction of all data.** |
| **4 Personnel Security** (For requirements please see Appendix C – Personnel Security) |
| 1. Have all staff who will have access to, or come into contact with, HMRC data or assets undergone Baseline Personnel Security Standard checks as a minimum?
 |
| **Yes** |
| 1. 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, including training and the specific nature of the HMRC contract.
 |
| **Onboarding / Briefing program undertaken by all staff by the Transform Delivery Lead.** |
| **5 Process Security** (For requirements please see Appendix D – Process Security) |
| 1. Please provide details of the format (e.g. electronic or paper) in which HMRC data will be held, how you will ensure segregation of HMRC data from other client's data, and the locations where this data will be processed.
 |
| **Electronic data only. Work undertaken within HMRC environment using “@digital.hmrc.gov.uk” accounts. Account management assets (contracts etc.) stored with Transform SharePoint with access restricted as per previous responses.** |
| 1. 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.
 |
| **Understood.** |
| 1. HMRC Data must not be offshored without the express permission of HMRC. ‘Offshoring’ means transferring the data outside of the UK, including by **storing it or accessing it** outside of the UK.

If you are considering offshoring HMRC data, please provide details on where and how you will ensure it is secure |
| * Will you be offshoring HMRC data? Yes ☐ No ☒
* Will you be offshoring HMRC Personal data? Yes ☐ No ☒
* Please list the country/countries you intend to ‘process’ (for example, store/access) HMRC data in
 |
| **Not applicable.** |
| 1. Will you be offshoring the Personal Data shared by HMRC to a non-adequate country? Yes ☐No ☒

(A list of countries covered by adequacy regulations can be found here) Please state the non-adequate country/countries here |
| **Not applicable.** |
| 1. Will you be processing (i.e., store/access) HMRC personal data in the US? Yes ☐ No ☒
2. If ‘yes’, has your organisation signed up to the UK Extension of the Data Privacy Framework? Yes ☐ No ☐
3. If no, please provide an explanation as to why your organisation has not signed up;
 |
| **Not applicable.** |
| 1. What do you consider your organisation under this contract:
* Data controller Yes ☐ No ☐
* Data processor Yes ☐ No ☒
* Joint Data controller Yes ☐ No ☐

Please explain why you made this determination |
| **Dictated by contract and consistent outline of UK Data Protection Act 2018** |
| 1. Please provide details of the protections and safeguards which would be applied and how it would be ensured 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.
 |
| * **Employee workstations including laptops are encrypted**
* **Security awareness training includes practices for secure remote working, such as ensuring physical device security and preventing visual eavesdropping**
* **A defence in depth approach is leveraged by layering various administrative, physical, and technical controls to protect valuable assets.**
* **Hardware firewalls exist at network perimeters and are configured to deny by default.**
* **Intrusion Prevention Systems have been implemented to mitigate advanced persistent threats.**
* **A centrally managed anti-virus and anti-malware solution has been implemented on Transform information systems including servers and workstations.**
* **E-mail hygiene solutions have been implemented to mitigate attack vectors originating from e-mail messages.**
* **A Data Loss Prevention system has been implemented to prevent sensitive data from being sent via email.**
* **Transform leverages TLS 1.2 and AES-256 encryption wherever feasible to protect sensitive data in transit.**
* **Data is logically segregated to ensure proper information containerization.**
* **Backups of critical systems are scheduled daily, encrypted, and routinely tested. #**
* **Production and non-production environments are segregated to ensure the proper segregation of duties for data access.**
* **Production data is prohibited from being removed from production environments.**
* **Retention and deletion of all data follows Transform’s policies assuring client contractual, legal, and regulatory requirements for data disposal are followed.**
 |
| 1. If your organisation is located or have servers or staff in a location outside the UK, where personal data will be received or accessed from, and this country is considered to be a non-adequate country, HMRC will need to undertake a Transfer Risk Assessment on each non-adequate country the data will be received or accessed from. Where this is the case, please complete the questions in Appendix F for each non-adequate country.
 |
| **Not applicable.** |
| 1. If you intend to use a processor/sub-processor who are located, outside the UK, where personal data will be received or accessed from, and this country is considered to be a non-adequate country, please state the legal transfer mechanism you are using to conduct the restricted transfer. If you are using an appropriate safeguard under Article 46 of the UK GDPR, you will need to provide HMRC with a copy of the Transfer Risk Assessment you have completed for your processor/sub-processor.
 |
| **Not applicable.** |
| 1. Subject to HMRC's assessment of the aforementioned information, HMRC reserves the right to reject a bidder’s entire tender submission and/or terminate any contract awarded
 |
| * 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.
 |
| **As above.** |
| 1. What arrangements are in place for secure disposal of HMRC assets that may be in your possession once no longer required?
 |
| **Retention and deletion of all data follows Transform’s policies assuring client contractual, legal, and regulatory requirements for data disposal.** |
| 1. How will you advise HMRC of security incidents that impact HMRC assets that may be in your possession?
 |
| **As stipulated within the contract – by email, as soon as we are aware of the issue, to the nominated HMRC contact.** |
| **6 Business Continuity** |
| Please provide an overview of your organisation’s business continuity and disaster recovery plans in terms of HMRC data under the Contract or attach a copy of your Business Continuity and Disaster Recovery Plans. 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. |
| **We classify our Business Continuity and Disaster Recovery Plans as Confidential however:*** **Business Continuity and Disaster Recovery Plans have been established to ensure the quick and prioritized recovery of services following a disaster.**
* **Business Continuity and Disaster Recovery Plans are tested in a live or table-top exercise at least annually.**
* **Transform has a rigorous technology standard and methodology based on redundancy and high availability, including:**
	+ **Redundancy and high availability by design throughout the IT infrastructure, eliminating single points of failure, especially for the core/central IT shared services and dependencies.**
	+ **N+1 component redundancy in either active-passive or active-active configuration.**
	+ **Geographically segregated facilities/computing locations.**
	+ **Service provider and supplier diversity.**
	+ **Network pathway and carrier diversity.**
	+ **Investing in and implementing technology platforms that are**
	+ **recognized as best-of-breed within their service areas, and which**
	+ **include robust feature sets suitable for high availability.**
	+ **Adopting as part of overall IT strategy the following tactics:**

**1. use of cloud services from best-of-breed providers that maintain their own robust standards for availability, assured by audit reports and backed by service level guarantees.** **2. use of private cloud and virtualization within Transformmanaged solutions, including portability/replication of systems, platforms, data, and services as a required function.** **3. remote working –enabling the ability for staff to work and connect remotely at multiple entry points into the network and for online services.*** **Transform is a fully work-from-home capable organisation and all staff are trained on effective ‘work from home’ capabilities.**
 |

**The following appendices provide additional information on the types of security control that may 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** |
| --- | --- | --- |
| Physical Access - secure areas | Visitors limited to those with a business need, issued with identifying badges upon arrival and escorted at all times. | Visitor to be issued with identifying badges upon arrival. A visitor log maintained and visitors sign-in and out. |
| Building | Constructed of robust building materials typically, brick or lightweight block walls.External doors of solid construction, locked during silent hours. 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. | Lockable double glazed or similar unit. Emergency exit doors included on intruder detection system.Security Keys should not be removed from the premises.Intruder alarm with keyholder response. |
| 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 | Adequate lockable storage for HMRC material.Material transported using previously agreed processes with HMRC. | Point to point transfer of material in locked containers. |

**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. |
| Authorisation | Users and Administrators must be authorised to use the System/Service. |  |
| Authentication[[1]](#footnote-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. |  |
| Malware Protection[[2]](#footnote-2) | Controls such as anti-virus software must detect and prevent infection by known malicious code.3 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.Application code development should be tightly controlled and subject to strict quality control to reduce the potential for insertion of backdoors that could be exploited by an attackerFor 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. |
| Network Security | Boundary controls should have content checking and a blocking policy in place e.g. firewalls. | 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 the Security Policy Framework in an agreed process with HMRC. |  |
| 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[[3]](#footnote-3). 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. | See www.gov.uk specifically the link to the Disclosure & Barring Service for more information. |
| Confidentiality Agreements | Confidentiality Agreements (CA) must be completed by all staff with potential or actual access to HMRC information assets as requested. | HMRC’s Commercial Directorate can supply the template form. |

**Appendix D – Process Security**

| **Process Security**  | **Requirements** | **Recommended** |
| --- | --- | --- |
| Security Policies, Processes and Procedures | 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.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. | Assets, especially information assets must be destroyed when no longer required so that they cannot be reconstituted or reused by an unauthorised third party. Shedding is recommended. Electronic files should be weeded and deleted when no longer required. |
| 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. |  |

**Appendix E – Business Continuity**

| **Business Continuity** | **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. |  |

12. **AUTHORITY’S MANDATORY TERMS**

1. For the avoidance of doubt, references to ‘the Agreement’ means Call-Off Contract reference SR2368360228 between the Supplier and the Authority. References to ‘the Authority’ mean ‘the Buyer’ (the Commissioners for His Majesty’s Revenue and Customs).
2. The Agreement incorporates the Authority’s mandatory terms set out in this Schedule 1.
3. In case of any ambiguity or conflict, the Authority’s mandatory terms in this Schedule 1will supersede any other terms in the Agreement.
4. For the avoidance of doubt, the relevant definitions for the purposes of the defined terms set out in the Authority’s mandatory terms in this Schedule 1 are the definitions set out at Clause 1 below.
5. **Definitions**

|  |  |
| --- | --- |
| **“Affiliate”** | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time; |
| **“Authority Data”** | 1. 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:
	* + 1. supplied to the Supplier by or on behalf of the Authority; and/or
			2. which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or
2. 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;
 |
| **“Charges”**  | the charges for the Services as specified in Schedule 2. |
| **“Connected Company”** | means, in relation to a company, entity or other person, the Affiliates of that company, entity or other person or any other person associated with such company, entity or other person; |
| **“Control”** | the possession by a person, directly or indirectly, of the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and “Controls” and “Controlled” shall be interpreted accordingly; |
| **“Controller”, “Processor”, “Data Subject”,** | take the meaning given in the UK GDPR;  |
| **“Data Protection Legislation”** | * 1. "the data protection legislation" as defined in section 3(9) of the Data Protection Act 2018; and;
	2. all applicable Law about the processing of personal data and privacy;
 |
| **“Key Subcontractor”** | any Subcontractor:1. which, in the opinion of the Authority, performs (or would perform if appointed) a critical role in the provision of all or any part of the Services; and/or
2. with a Subcontract with a contract value which at the time of appointment exceeds (or would exceed if appointed) ten per cent (10%) of the aggregate Charges forecast to be payable under this Call-Off Contract;
 |
| **“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; |
| **“Personal Data”** | has the meaning given in the UK GDPR;  |
| **“Purchase Order Number”**  | the Authority’s unique number relating to the supply of the Services;   |
| **“Services”**  | the services to be supplied by the Supplier to the Authority under the Agreement, including the provision of any Goods; |
| **“Subcontract”** | any contract or agreement (or proposed contract or agreement) between the Supplier (or a Subcontractor) and any third party whereby that third party agrees to provide to the Supplier (or the Subcontractor) all or any part of the Services, or facilities or services which are material for the provision of the Services, or any part thereof or necessary for the management, direction or control of the Services or any part thereof; |
| **“Subcontractor”** | any third party with whom:1. the Supplier enters into a Subcontract; or
2. a third party under (a) above enters into a Subcontract,

or the servants or agents of that third party; |
| **“Supplier Personnel”** | all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier’s obligations under the Agreement;  |
| **“Supporting Documentation”** | sufficient information in writing to enable the Authority to reasonably verify the accuracy of any invoice;  |
| **“Tax”** | 1. all forms of tax whether direct or indirect;
2. national insurance contributions in the United Kingdom and similar contributions or obligations in any other jurisdiction;
3. 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
4. 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; |
| **“Tax Non-Compliance”** | where an entity or person under consideration meets all 3 conditions contained in the relevant excerpt from HMRC’s “Test for Tax Non-Compliance”, as set out in Annex 1, where:1. the “Economic Operator” means the Supplier or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause 4.3; and
2. any “Essential Subcontractor” means any Key Subcontractor;
 |
| **“UK GDPR”**  | the UK General Data Protection Regulation, the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679); |
| **“VAT”** | value added tax as provided for in the Value Added Tax Act 1994. |

1. **Payment and Recovery of Sums Due**

## The Supplier shall invoice the Authority as specified in Part A – Order Form of the Agreement. Without prejudice to the generality of the invoicing procedure specified in the Agreement, the Supplier shall procure a Purchase Order Number from the Authority prior to the commencement of any Services and the Supplier acknowledges and agrees that should it commence Services without a Purchase Order Number:

### the Supplier does so at its own risk; and

### the Authority shall not be obliged to pay any invoice without a valid Purchase Order Number having been provided to the Supplier.

* 1. Each invoice and any Supporting Documentation required to be submitted in accordance with the invoicing procedure specified in the Agreement shall be submitted by the Supplier, as directed by the Authority from time to time via the Authority’s electronic transaction system.
	2. If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Authority.  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.
1. **Warranties**
	1. The Supplier represents and warrants that:
		1. in the three years prior to the Effective Date, it has been in full compliance with all applicable securities and Laws related to Tax in the United Kingdom and in the jurisdiction in which it is established;
		2. it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and
		3. no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the 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 the Supplier has notified the Authority of any profit warnings issued in respect of the Supplier in the three years prior to the Effective Date.
	2. If at any time the Supplier becomes aware that a representation or warranty given by it under Clause 3.1.1, 3.1.2 and/or 3.1.3 has been breached, is untrue, or is misleading, it shall immediately notify the Authority of the relevant occurrence in sufficient detail to enable the Authority to make an accurate assessment of the situation.
	3. In the event that the warranty given by the Supplier pursuant to Clause 3.1.2 is materially untrue, the Authority shall be entitled to terminate the Agreement pursuant to the Call-Off clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).
2. **Promoting Tax Compliance**
	1. All amounts stated are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Authority following delivery of a valid VAT invoice.
	2. To the extent applicable to the Supplier, the Supplier shall at all times comply with all Laws relating to Tax and with the equivalent legal provisions of the country in which the Supplier is established.
	3. The Supplier shall provide to the Authority the 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 Subcontractor of the Supplier prior to the provision of any material Services under the Agreement by that agent, supplier or Subcontractor. Upon a request by the Authority, the Supplier shall not contract, or will cease to contract, with any agent, supplier or Subcontractor supplying Services under the Agreement.
	4. If, at any point during the Term, there is Tax Non-Compliance, the Supplier shall:
		1. notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and
		2. promptly provide to the Authority:
3. details of the steps which the Supplier is taking to resolve the Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and
4. such other information in relation to the Tax Non-Compliance as the Authority may reasonably require.
	1. The Supplier shall indemnify the Authority on a continuing basis 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 4.5 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.
	2. Upon the Authority’s request, the Supplier shall provide (promptly or within such other period notified by the Authority) information which demonstrates how the Supplier complies with its Tax obligations.
	3. If the Supplier:
		1. fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with Clauses 4.2, 4.4.1 and/or 4.6 this shall be a material breach of the Agreement;
		2. fails to comply (or if the Authority receives information which demonstrates to it that the Supplier has failed to comply) with a reasonable request by the Authority that it must not contract, or must cease to contract, with any agent, supplier or Subcontractor of the Supplier as required by Clause 4.3 on the grounds that the agent, supplier or Subcontractor of the Supplier is involved in Tax Non-Compliance this shall be a material breach of the Agreement; and/or
		3. fails to provide details of steps being taken and mitigating factors pursuant to Clause 4.4.2 which in the reasonable opinion of the Authority are acceptable this shall be a material breach of the Agreement;

and any such material breach shall allow the Authority to terminate the Agreement pursuant to the Call-Off Clause which provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).

* 1. The Authority may internally share any information which it receives under Clauses 4.3 to 4.4 (inclusive) and 4.6, for the purpose of the collection and management of revenue for which the Authority is responsible.
1. **Use of Off-shore Tax Structures**
	1. Subject to the principles of non-discrimination against undertakings based either in member countries of the European Union or in signatory countries of the World Trade Organisation Agreement on Government Procurement, the Supplier shall not, and shall ensure that its Connected Companies, Key Subcontractors (and their respective Connected Companies) shall not, have or put in place (unless otherwise agreed with the Authority) any arrangements involving the use of off-shore companies or other off-shore entities the main purpose, or one of the main purposes, of which is to achieve a reduction in United Kingdom Tax of any description which would otherwise be payable by it or them on or in connection with the payments made by or on behalf of the Authority under or pursuant to this Agreement or (in the case of any Key Subcontractor and its Connected Companies) United Kingdom Tax which would be payable by it or them on or in connection with payments made by or on behalf of the Supplier under or pursuant to the applicable Key Subcontract (**“Prohibited Transactions”**). Prohibited Transactions shall not include transactions made between the Supplier and its Connected Companies or a Key Subcontractor and its Connected Companies on terms which are at arms-length and are entered into in the ordinary course of the transacting parties’ business.
	2. The Supplier shall notify the Authority in writing (with reasonable supporting detail) of any proposal for the Supplier or any of its Connected Companies, or for a Key Subcontractor (or any of its Connected Companies), to enter into any Prohibited Transaction. The Supplier shall notify the Authority within a reasonable time to allow the Authority to consider the proposed Prohibited Transaction before it is due to be put in place.
	3. In the event of a Prohibited Transaction being entered into in breach of Clause 5.1 above, or in the event that circumstances arise which may result in such a breach, the Supplier and/or the Key Subcontractor (as applicable) shall discuss the situation with the Authority and, in order to ensure future compliance with the requirements of Clauses 5.1 and 5.2, the Parties (and the Supplier shall procure that the Key Subcontractor, where applicable) shall agree (at no cost to the Authority) timely and appropriate changes to any such arrangements by the undertakings concerned, resolving the matter (if required) through the escalation process in the Agreement.
	4. Failure by the Supplier (or a Key Subcontractor) to comply with the obligations set out in Clauses 5.2 and 5.3 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).
2. **Data Protection and off-shoring**
	1. The parties agree that the Supplier shall, whether it is the Controller or Processor, in relation to any Personal Data processed in connection with its obligations under the Agreement:
		1. not process or permit to be processed Personal Data outside of the United Kingdom unless the prior explicit written consent of the Authority has been obtained and the following conditions are fulfilled:
	2. the Supplier or any applicable Processor has provided appropriate safeguards in relation to any transfer of the Personal Data (whether in accordance with UK GDPR Article 46 or, where relevant, section 75 of the Data Protection Act 2018) as determined by either the Authority or the Supplier when it is the Controller;
	3. the Data Subject has enforceable rights and effective legal remedies;
	4. the Supplier or any applicable Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is processed (or, if it is not so bound, uses its best endeavours to assist either the Authority or the Supplier when it is the Controller in meeting its obligations); and
	5. the Supplier or any applicable Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
	6. Failure by the Supplier to comply with the obligations set out in Clause 6.1 shall allow the Authority to terminate the Agreement pursuant to the Clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause or equivalent clause).
3. **Commissioners for Revenue and Customs Act 2005 and related Legislation**
	1. The Supplier shall comply with and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in Section 18 of the Commissioners for Revenue and Customs Act 2005 (‘CRCA’) 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 19 of CRCA.
	2. The Supplier shall comply with and shall ensure that all Supplier Personnel who will have access to, or are provided with, Authority Data comply with the obligations set out in 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.
	3. The Supplier shall regularly (not less than once every six (6) months) remind all Supplier Personnel who will have access to, or are provided with, Authority Data in writing of the obligations upon Supplier Personnel set out in Clause 7.1 above. The Supplier shall monitor the compliance by Supplier Personnel with such obligations.
	4. 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 Confidentiality Declaration, in the form provided at Annex 2. The Supplier shall provide a copy of each such signed declaration to the Authority upon demand.
	5. In the event that the Supplier or the Supplier Personnel fail to comply with this Clause 7, the Authority reserves the right to terminate the Agreement with immediate effect pursuant to the clause that provides the Authority the right to terminate the Agreement for Supplier fault (termination for Supplier cause).

**Annex 1**

**Excerpt from HMRC’s “Test for Tax Non-Compliance”**

*Condition one (An in-scope entity or person)*

1. There is a person or entity (“X”) which is either:
2. The Economic Operator or Essential Subcontractor (“EOS”);
3. Part of the same group of companies as EOS. An entity will be treated as within the same group of EOS where that entities’ financial statements would be required to be consolidated with those of EOS if prepared in accordance with *IFRS 10 Consolidated Financial Accounts[[4]](#footnote-4)*;
4. Any director, shareholder or other person (“P”) which exercises control over EOS. ‘Control’ means P can secure, through holding of shares or powers under articles of association or other document that EOS’s affairs are conducted in accordance with P’s wishes.

*Condition two (Arrangements involving evasion, abuse or tax avoidance)*

1. X has been engaged in one or more of the following:
	1. Fraudulent evasion[[5]](#footnote-5);
	2. Conduct caught by the General Anti-Abuse Rule[[6]](#footnote-6);
	3. Conduct caught by the Halifax Abuse principle[[7]](#footnote-7);
	4. Entered into arrangements caught by a DOTAS or VADR scheme[[8]](#footnote-8);
	5. Conduct caught by a recognised ‘anti-avoidance rule’[[9]](#footnote-9) being a statutory provision which targets arrangements where either a main purpose, or an expected benefit, is to obtain a tax advantage or where the arrangement is not effected for commercial purposes. ‘Targeted Anti-Avoidance Rules’ (TAARs). It may be useful to confirm that the Diverted Profits Tax is a TAAR for these purposes;
	6. Entered into an avoidance scheme identified by HMRC’s published Spotlights list[[10]](#footnote-10);
	7. Engaged in conduct which falls under rules in other jurisdictions which are equivalent or similar to (a) to (f) above.

*Condition three (Arrangements are admitted, or subject to litigation/prosecution or identified in a published list (Spotlights))*

1. X’s activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:
	1. In respect of 2(a), either X:
2. Has accepted the terms of an offer made under a Contractual Disclosure Facility (“CDF”) pursuant to the Code of Practice 9 (COP9) procedure[[11]](#footnote-11); or,
3. Has been charged with an offence of fraudulent evasion.
	1. In respect of 2(b) to (e), once X has commenced the statutory appeal process by filing a Notice of Appeal and the appeal process is ongoing including where the appeal is stayed or listed behind a lead case (either formally or informally). NB: Judicial reviews are not part of the statutory appeal process and no supplier would be excluded merely because they are applying for judicial review of an HMRC or HMT decision relating to tax or national insurance.
	2. In respect of 2(b) to (e), during an HMRC enquiry, if it has been agreed between HMRC and X that there is a pause with the enquiry in order to await the outcome of related litigation.
	3. In respect of 2(f) this condition is satisfied without any further steps being taken.
	4. In respect of 2(g) the foreign equivalent to each of the corresponding steps set out above in 3(a) to (c).

For the avoidance of doubt, any reference in this Annex 1 to any Law includes a reference to that Law as amended, extended, consolidated or re‑enacted from time to time including any implementing or successor legislation.

**Annex 2 Form**

**CONFIDENTIALITY DECLARATION**

CONTRACT REFERENCE: SR2368360228 1 April 2025

DECLARATION:

I solemnly declare that:

1. I am aware that the duty of confidentiality imposed by section 18 of the Commissioners for Revenue and Customs Act 2005 applies to Authority Data (as defined in the Agreement) that has been or will be provided to me in accordance with the Agreement.
2. I understand and acknowledge that under Section 19 of the Commissioners for Revenue and Customs Act 2005 it may be a criminal offence to disclose any Authority Data provided to me.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

**Appendix F - Transfer Risk Assessment – Not applicableAppendix 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.

### **ANNEX 1: Request for Services (RFS)**

1. Buyer Requirements

|  |  |
| --- | --- |
| **Date of Request for Services RFS:**  |   |
| **RFS Reference:**  |  |
| **Buyer:**  |  |
| **Supplier:**  |  |
| **Requirements:**  |  |

|  |  |
| --- | --- |
|  |  |
| **Milestones:**  |  |
| **Start Date:**  |  |
| **Completion Date:**  |  |
| **Charging Method(s)**  | Choose an item: * Capped time and materials (CTM) ☐
* Time and materials (T&M) ☐
* Fixed price ☐
* Other pricing method or a combination of pricing methods agreed by the Parties (*please define ‘other method’ below*) ☐

 * Other pricing method: …………………………………………….
 |

1. RFS Content

* The RFS should also include a summary of the total value of this RFS

* Multiple RFSs can operate concurrently.

* The Supplier will keep accurate records of the time spent by the Supplier staff in providing the services and will provide records to the Buyer for inspection upon request.

* For any additional work over and above the effort specified for this RFS, the Parties will execute separate RFSs for each work package.

* The rights, obligations and details agreed by the Parties and set out in this RFS apply only in relation to the Services that are to be delivered under this RFS and will not apply to any other RFSs executed or to be executed under this Call-Off Contract unless otherwise agreed by the Parties.
* Where an RFS covers a delivery that will transition into business as usual, the Supplier will transparently document to the Buyer any impact to the baseline service/pricing, and the relevant documentation will be varied for such provision.

* 1. Supplier Proposal

For the provision of the deliverables as outlined in Section 1 above, the Supplier will provide a proposal outlining their approach to delivery, and a formal quotation (including a breakdown of the proposed costs), below:

HMRC Online Trade Tariff SR730006772

|  |
| --- |
| **Supplier Proposal:**  |
|  |
| **Cost:**  |
|

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Day rate**  |  |  |  |  | **Total days**  | **Cost**  |
| **# days in month**  | -  | - | - | - | - | -  | -  |

  |
| **Date Provided:**  |
|  |

22

OFFICIAL

* 1. Agreement of the RFS

**By signing this RFS, the Parties agree to be bound by the terms and conditions set out herein:**

|  |  |  |
| --- | --- | --- |
|   | For and on behalf of the Supplier  | For and on behalf of the Buyer  |
| Name:  |  |  |
| Title:  |  |  |
| Signature:  |  |  |
| Date:  |  |  |

## Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier’s Digital Marketplace pricing document) can’t be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

* 1. Ancillary costs:
	2. In order to support the service on an ongoing/day-to-day basis, the following tools are required, and estimated monthly charges will be provided by the Supplier
	3. Any new projects being transitioned into the service (i.e. new scope) or a significant change to current service (i.e. change of scope) should trigger a review of the below table and an update of applicable ancillary costs to the current estimates and unit costs.
	4. Unit costs are set by the service provider. Transform will provide a forecast and an actual for supplier costs and pass these onto HMRC directly each month.

***Notes:***

* + 1. *Unit charges are subject to change, as per the contractual terms between the Supplier and their Subcontractors.*
		2. *AWS and New Relic costs are subject to Buyer consumption, and therefore the amount charged on the monthly invoice will fluctuate to reflect consumption.*

**1.2.** Time and Materials (or Fixed Price if applicable):

a) The table below provides a breakdown of the roles required, their associated day-rates, and the expected activities performed by Supplier personnel, associated with the successful execution of the Services

## Schedule 3: Collaboration agreement – NOT USED

## Schedule 4: Alternative clauses – NOT USED

##

## Schedule 5: Guarantee – NOT USED

##

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

|  |  |
| --- | --- |
| **Expression** | **Meaning** |
| **Additional Services** | Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request. |
| **Admission Agreement** | The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s). |
| **Application** | The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform). |
| **Audit** | An audit carried out under the incorporated Framework Agreement clauses. |
| **Background IPRs** | For each Party, IPRs:* owned by that Party before the date of this Call-Off Contract

(as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes* created by the Party independently of this Call-Off Contract, or

For the Buyer, Crown Copyright which isn’t available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software. |
| **Buyer** | The contracting authority ordering services as set out in the Order Form. |
| **Buyer Data** | All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer. |
| **Buyer Personal Data** | The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract. |
| **Buyer Representative** | The representative appointed by the Buyer under this Call-Off Contract. |

|  |  |
| --- | --- |
|  **Buyer Software** | Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services. |
| **Call-Off Contract** | This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement. |
| **Charges** | The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract. |
| **Collaboration Agreement** | An agreement, substantially in the form, set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer’s Services and to ensure that the Buyer receives end-to-end services across its IT estate. |
| **Commercially Sensitive** **Information** | Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive. |
| **Confidential Information** | Data, Personal Data and any information, which may include (but isn’t limited to) any:* information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above
* other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
 |
| **Control** | ‘Control’ as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly. |
| **Controller** | Takes the meaning given in the UK GDPR. |
| **Crown** | The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf. |

|  |  |
| --- | --- |
|  **Data Loss Event** | Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach. |
| **Data Protection Impact** **Assessment (DPIA)** | An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data. |
| **Data Protection** **Legislation (DPL)** | (i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy. |
| **Data Subject** | Takes the meaning given in the UK GDPR |
| **Default** | Default is any:* breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)
* other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract

Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer. |
| **DPA 2018** | Data Protection Act 2018. |
| **Employment Regulations** | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) (‘TUPE’) . |
| **End** | Means to terminate; and Ended and Ending are construed accordingly. |
| **Environmental****Information Regulations or EIR** | The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the InformationCommissioner or relevant government department about the regulations. |
| **Equipment** | The Supplier’s hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract. |

|  |  |
| --- | --- |
|  **ESI Reference Number** | The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool. |
| **Employment Status** **Indicator test tool or ESI tool** | The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here:https://www.gov.uk/guidance/check-employment-status-fortax |
| **Expiry Date** | The expiry date of this Call-Off Contract in the Order Form. |
| **Financial Metrics** | The following financial and accounting measures:* Dun and Bradstreet score of 50
* Operating Profit Margin of 2%
* Net Worth of 0
* Quick Ratio of 0.7
 |
| **Force Majeure** | A force Majeure event means anything affecting either Party's performance of their obligations arising from any:* acts, events or omissions beyond the reasonable control of the affected Party
* riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare
* acts of government, local government or Regulatory Bodies
* fire, flood or disaster and any failure or shortage of power or fuel
* industrial dispute affecting a third party for which a substitute third party isn’t reasonably available

The following do not constitute a Force Majeure event:* any industrial dispute about the Supplier, its staff, or failure in the Supplier’s (or a Subcontractor's) supply chain
* any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure
* the event was foreseeable by the Party seeking to rely on Force

Majeure at the time this Call-Off Contract was entered into* any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
 |
| **Former Supplier** | A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor). |
| **Framework Agreement** | The clauses of framework agreement RM1557.14 together with the Framework Schedules. |
| **Fraud** | Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown. |

|  |  |
| --- | --- |
| **Freedom of Information** **Act or FoIA** | The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation. |
| **G-Cloud Services** | The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement. |
| **UK GDPR** | The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679). |
| **Good Industry Practice** | Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances. |
| **Government****Procurement Card** | The government’s preferred method of purchasing and payment for low value goods or services. |
| **Guarantee** | The guarantee described in Schedule 5. |
| **Guidance** | Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence. |
| **Implementation Plan** | The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding. |
| **Indicative test** | ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6. |
| **Information** | Has the meaning given under section 84 of the Freedom of Information Act 2000. |

|  |  |
| --- | --- |
|  **Information security management system** | The information security management system and process developed by the Supplier in accordance with clause 16.1. |
| **Inside IR35** | Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool. |

|  |  |
| --- | --- |
| **Insolvency event** | Can be:* a voluntary arrangement
* a winding-up petition
* the appointment of a receiver or administrator
* an unresolved statutory demand
* a Schedule A1 moratorium
* a Supplier Trigger Event
 |
| **Intellectual Property** **Rights or IPR** | Intellectual Property Rights are:(a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information(b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction* (c) all other rights having equivalent or similar effect in any country or jurisdiction
 |
| **Intermediary** | For the purposes of the IR35 rules an intermediary can be:* the supplier's own limited company
* a service or a personal service company
* a partnership

It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency). |
| **IPR claim** | As set out in clause 11.5. |
| **IR35** | IR35 is also known as ‘Intermediaries legislation’. It’s a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary. |
| **IR35 assessment** | Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35. |

|  |  |
| --- | --- |
| **Know-How** | All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier’s or Buyer’s possession before the Start date. |
| **Law** | Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply. |
| **Loss** | All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgement, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly. |
| **Lot** | Any of the 3 Lots specified in the ITT and Lots will be construed accordingly. |
| **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. |
| **Management Charge** | The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract. |
| **Management Information** | The management information specified in Framework Agreement Schedule 6. |
| **Material Breach** | Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract. |
| **Ministry of Justice Code** | The Ministry of Justice’s Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000. |

|  |  |
| --- | --- |
| **New Fair Deal** | The revised Fair Deal position in the HM Treasury guidance: “Fair Deal for staff pensions: staff transfer from central government” issued in October 2013 as amended. |
| **Order** | An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes. |
| **Order Form** | The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services. |
| **Ordered G-Cloud** **Services** | G-Cloud Services which are the subject of an order by the Buyer. |
| **Outside IR35** | Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool. |
| **Party** | The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly. |
| **Performance Indicators** | The performance information required by the Buyer from the Supplier set out in the Order Form. |
| **Personal Data** | Takes the meaning given in the UK GDPR. |
| **Personal Data Breach** | Takes the meaning given in the UK GDPR. |
| **Platform** | The government marketplace where Services are available for Buyers to buy. |
| **Processing** | Takes the meaning given in the UK GDPR. |
| **Processor** | Takes the meaning given in the UK GDPR. |
| **Prohibited act** | To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:* induce that person to perform improperly a relevant function or activity
* reward that person for improper performance of a relevant function or activity
* commit any offence:
	+ under the Bribery Act 2010
	+ under legislation creating offences concerning Fraud
	+ at common Law concerning Fraud
	+ committing or attempting or conspiring to commit Fraud
 |

|  |  |
| --- | --- |
|  **Project Specific IPRs** | Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier’s Background IPRs. |
| **Property** | Assets and property including technical infrastructure, IPRs and equipment. |
| **Protective Measures** | Appropriate technical and organisational measures which may include: pseudonymisation 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 such measures adopted by it. |
| **PSN or Public Services** **Network** | The Public Services Network (PSN) is the government’s high performance network which helps public sector organisations work together, reduce duplication and share resources. |
| **Regulatory body or bodies** | Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract. |
| **Relevant person** | Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body. |
| **Relevant Transfer** | A transfer of employment to which the employment regulations applies. |
| **Replacement Services** | Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party. |
| **Replacement supplier** | Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer). |
| **Security management plan** | The Supplier's security management plan developed by the Supplier in accordance with clause 16.1. |

|  |  |
| --- | --- |
|  **Services** | The services ordered by the Buyer as set out in the Order Form. |
| **Service Data** | Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data and Performance Indicators data. |
| **Service definition(s)** | The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn’t limited to, those items listed in Clause 2 (Services) of the Framework Agreement. |
| **Service description** | The description of the Supplier service offering as published on the Platform. |
| **Service Personal Data** | The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract. |
| **Spend controls** | The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see [https://www.gov.uk/service-manual/agile-delivery/spend-controlsche ck-if-you-need-approval-to-spend-money-on-a-service](https://protect.checkpoint.com/v2/r06/___https%3A//www.gov.uk/xjwAnhj-rfszfqdflnqj-ijqnAjwDdxujsi-htsywtqx-hmjhp-nk-Dtz-sjji-fuuwtAfq-yt-xujsi-rtsjD-ts-f-xjwAnhj___.ZXV3MjpuZXh0MTU6YzpvOmU5MmFmMDc4NjFhMThmY2EyM2YwYjNmMWJhZDE2MThkOjc6NDY3Nzo2ZjkwMDYyMDExYTM2NjRkZGUyNTFiMjBjZmIyNDBiYjI2NWFlMWNmOTM2NWM4ZTE1ZDgxOWY4NzdlMDk1MTQxOnA6VDpU)  |
| **Start date** | The Start date of this Call-Off Contract as set out in the Order Form. |
| **Subcontract** | Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof. |
| **Subcontractor** | Any third party engaged by the Supplier under a subcontract(permitted under the Framework Agreement and the Call-OffContract) and its servants or agents in connection with the provision of G-Cloud Services. |
| **Subprocessor** | Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract. |
| **Supplier** | The person, firm or company identified in the Order Form. |
| **Supplier Representative** | The representative appointed by the Supplier from time to time in relation to the Call-Off Contract. |

|  |  |
| --- | --- |
| **Supplier staff** | All persons employed by the Supplier together with the Supplier’s servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract. |
| **Supplier Terms** | The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier’s Application. |
| **Term** | The term of this Call-Off Contract as set out in the Order Form. |
| **Trigger Event** | The Supplier simultaneously fails to meet three or more Financial Metrics for a period of at least ten Working Days. |
| **Variation** | This has the meaning given to it in clause 32 (Variation process). |
| **Variation Impact Assessment** | An assessment of the impact of a variation request by the Buyer completed in good faith, including:* 1. details of the impact of the proposed variation on the Deliverables and the Supplier's ability to meet its other obligations under the Call-Off Contract;
	2. details of the cost of implementing the proposed variation;
	3. details of the ongoing costs required by the proposed variation 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;
	4. a timetable for the implementation, together with any proposals for the testing of the variation; and

such other information as the Buyer may reasonably request in (or in response to) the variation request; |
| **Working Days** | Any day other than a Saturday, Sunday or public holiday in England and Wales. |
| **Year** | A contract year. |

### Intentionally Blank

## Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended

## Annex 1 - Processing Personal Data

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

* 1. The contact details of the Buyer’s Data Protection Officer are: advice.dpa@hmrc.gov.uk

1.2 The contact details of the Supplier’s Data Protection Officer are:

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

1.4 Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of Controller and Processor for each Category of Personal Data | **The Buyer is Controller and the Supplier is Processor**The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:* ***Basic Personal identifiers***
 |
| Duration of the Processing | The user's work email address will be retained while they require access to the service.Once a user no longer requires access, or if their access has been revoked, then their account will be deleted.If a registration has been unsuccessful, we will retain the user's details for up to 6 months before deletion. |
| Nature and purposes of the Processing | The personal data consists of the user's work email address which they enter as part of the registration process for the OTT developer hub, and the email address that they used to sign up for Government Gateway. The personal data is not sensitive. The email address is used to contact the user about their registration, and to notify them of any essential maintenance/tariff changes affecting their use of the service. Registrations are processed within 5 working days. The users are primarily UK based, but there may be instances where an organisation is using off-shore developers who may require access. The data is stored in the London region of AWS. GOV.UK Notify processes data in Ireland for sending emails. The existing Online Trade Tariff support mailbox used to send the notifications is part of HMRCs existing estate.At the time we collect the information, we inform the user that their details will only be used to send essential updates regarding the tool and their verification request. The data from the web form will be stored in the database, and also be received into the Online Trade Tariff support mailbox, with the content of the email clearly stating that the request is for API registration. We then use that information to process their registration, and the support ticket closed once that's completed so that it won't be further processed. From that point forward the user's data will only be accessible from the database. Should we need to send a notification to any/all users (which we expect to do only rarely) we would manually query the database for the relevant user records, and then manually send the notification through GOV.UK Notify.We do not validate the user's work email address. They can access their application using their Government Gateway account to check on the status. The user will be able to update their email address by contacting the support mailbox which will be then manually actioned by the development team. They will also be able to request for their account to be deleted via this method.The service consists of separate front-end web application and back-end API service, both implemented using NodeJS.These applications are deployed into AWS Elastic Container Storage. The back-end application is connected to an AWS DynamoDB database into which the data is stored. This is encrypted at rest. This is all deployed into an existing AWS platform which was built specifically to host the Online Trade Tariff applications. This platform has been designed and implemented according to the AWS well-architected base practices, and has been security tested by a third partyThe data is first time collected for this service - there is no reuse or repurposing of data collected other services/previous occasions nor is there any onward repurposing of the data collected. This processing is carried out by our external supplier, Transform, and is subject to the requirements and conditions of their supplier to HMRC contract. These include GDPR adherence (including purpose limitation), data breach liability and data retention periods. |
| Type of Personal Data | Work email addresses |
| Categories of Data Subject | Trade – customs agents, freight forwarders, hauliers. |
| International transfers and legal gateway | The data is stored in the London region of AWS. GOV.UK Notify processes data in Ireland for sending notification emails – usage and off-shoring agreement approved.Please note a full DPIA has been completed for this service:DPIA Report: Online Trade Tariff Developer HubReference ID: 15167Published Date: 04/08/2024 |
| Plan for return and destruction of the data once the Processing is complete | The user's work email address will be retained while they require access to the service.Once a user no longer requires access, or if their access has been revoked, then their account will be deleted.If a registration has been unsuccessful, we will retain the user's details for up to 6 months before deletion. |

## Schedule 8 (Corporate Resolution Planning) – NOT USED

## Schedule 9 - Variation Form

This form is to be used in order to change a Call-Off Contract in accordance with Clause 32 (Variation process)

|  |
| --- |
| **Contract Details**  |
| This variation is between: | **HM Revenue and Customs** name of Buyer] **(“the Buyer")**And **Transform UK Consulting Ltd** (**"the Supplier"**) |
| Contract name: | **Online Trade Tariff** name of contract to be changed] **(“the Contract”)** |
| Contract reference number: | SR2368360228  |
| **Details of Proposed Variation** |
| Variation initiated by: | Buyer/Supplier] |
| Variation number: |  |
| Date variation is raised: |  |
| Proposed variation |  |
| Reason for the variation: |  |
| A Variation Impact Assessment shall be provided within: |  |
| **Impact of Variation** |
| Likely impact of the proposed variation: | **Supplier to insert** assessment of impact |
| **Outcome of Variation** |
| Contract variation: | This Contract detailed above is varied as follows:* **[Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause]
 |
| Financial variation: | Original Contract Value: | £  |
| Additional cost due to variation: | £  |
| New Contract value: | £  |

1 This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by Buyer

2 Words and expressions in this Variation shall have the meanings given to them in the Contract.

3 The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.

Signed by an authorised signatory for and on behalf of the Buyer

|  |  |
| --- | --- |
| Signature |  |
| Date |  |
| Name (in Capitals) |  |
| Address |  |
|  |  |

Signed by an authorised signatory to sign for and on behalf of the Supplier

|  |  |
| --- | --- |
| Signature |  |
| Date |  |
| Name (in Capitals) |  |
| Address |  |

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). [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)
3. The term drives includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media and external hard drives. [↑](#footnote-ref-3)
4. https://www.iasplus.com/en/standards/ifrs/ifrs10 [↑](#footnote-ref-4)
5. ‘Fraudulent evasion’ means any ‘UK tax evasion offence’ or ‘UK tax evasion facilitation offence’ as defined by section 52 of the Criminal Finances Act 2017 or a failure to prevent facilitation of tax evasion under section 45 of the same Act. [↑](#footnote-ref-5)
6. “General Anti-Abuse Rule” means (a) the legislation in Part 5 of the Finance Act 2013; and (b) any

future legislation introduced into Parliament to counteract tax advantages arising from abusive

arrangements to avoid national insurance contributions [↑](#footnote-ref-6)
7. “Halifax Abuse Principle” means the principle explained in the CJEU Case C-255/02 Halifax and others [↑](#footnote-ref-7)
8. A Disclosure of Tax Avoidance Scheme (DOTAS) or VAT Disclosure Regime (VADR) scheme caught by rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Section 19 and Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Section 19 and Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992. [↑](#footnote-ref-8)
9. The full definition of ‘Anti-avoidance rule’ can be found at Paragraph 25(1) of Schedule 18 to the Finance Act 2016 and Condition 2 (a) above shall be construed accordingly. [↑](#footnote-ref-9)
10. Targeted list of tax avoidance schemes that HMRC believes are being used to avoid paying tax due and which are listed on the Spotlight website: https://www.gov.uk/government/collections/tax-avoidance-schemes-currently-in-the-spotlight [↑](#footnote-ref-10)
11. The Code of Practice 9 (COP9) is an investigation of fraud procedure, where X agrees to make a complete and accurate disclosure of all their deliberate and non-deliberate conduct that has led to irregularities in their tax affairs following which HMRC will not pursue a criminal investigation into the conduct disclosed. [↑](#footnote-ref-11)