



G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 Call-Off Contract

Part A: Order Form	2
Part B: Terms and conditions	14
Schedule 1: Services	41
Schedule 2: Call-Off Contract charges	42
Schedule 3: Collaboration agreement	42
Schedule 4: Alternative clauses	42
Schedule 5: Guarantee	42
Schedule 6: Glossary and interpretations	43
Schedule 7: UK GDPR Information	62
Annex 1: Processing Personal Data	
Schedule 8: Supplier Travel & Subsistence Policy	67
Schedule 9: HMRC Mandatory terms	73
Annex 2: (Signed Confidentiality Declaration)	84
Completed Security Plan Questionnaire.	85

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	2849 7146 4066 856
Call-Off Contract reference	HMRC PINS2023 Saadian
Call-Off Contract title	HMRC PINS service
Call-Off Contract description	Software supporting the PINS prison intelligence service managed by HMRC
Start date	1 st April 2023
Expiry date	31 st March 2026 with an option to extend for 1 single period of 12 months 01/04/26 – 31/3/27.
Call-Off Contract value	<p>£99,525</p> <p>plus a 1 year Optional extension for HMRC:</p> <p>Year 4: XXXXXXXXXX</p> <p>The optional extension will be subject to price indexation in line with the</p>

	<p>Government's Office for National Statistics stated Retail Price Index figure at the time.</p> <p>Total = £132,700</p> <p><u>Note1: Cloud Hosting Fees</u></p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
Charging method	BACS
Purchase order number	TBA

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

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	<p>HM Revenue & Customs (HMRC)</p> <p>100 Parliament Street,</p> <p>Westminster</p> <p>London</p> <p>SW1A 2BQ</p> <p>UK</p>
To the Supplier	<p>Saadian Technologies UK Ltd</p> <p>118 Pall Mall</p> <p>St. James's</p> <p>London</p> <p>SW1Y 5EA</p> <p>T: +44 (0) 207 157 9757</p> <p>Company number: Registered in England and Wales with 07180876 and in Ireland under 330243.</p>
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: [REDACTED]

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

For the Supplier:

Title: [REDACTED]

Name: [REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

Call-Off Contract term

Start date	This Call-Off Contract Starts on 1 st April 2023 and is valid for 36 months.
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least 30 Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>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).</p>

Extension period	<p>This Call-Off Contract can be extended by the Buyer for one period of up to 12 months, by giving the Supplier 1 months written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below.</p> <p>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.</p>
-------------------------	--

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	<p>This Call-Off Contract is for the provision of Services Under:</p> <p>Lot 2: Cloud software</p>
G-Cloud Services required	<p>The Services to be provided by the Supplier under the above Lot are outlined below:</p> <p>The PINS software provides prison data from NOMIS, enables HMRC to upload its own data and automatically cross references and links historic and current prisoner records.</p> <p>Daily monitoring of prison data allows PINS to send critical alerts and notifications to intelligence officers detailing key prisoner data changes as well as advance release notifications.</p>

	<p>Features of PINS version 5.1</p> <ul style="list-style-type: none"> - Provide a single view of an offender across multiple periods of custody - Add watches to prisoners for notifications of changes (including cell changes) or release - Search prison inmates by crime, nationality and prison location - Import and match current PPO/IOM lists from IDIOM or Excel - Track gang and organised crime nominals - Automatically match outstanding warrants - Bulk check any Excel list of offenders against prison inmates - Show clear visibility of historic and current cell and wing sharing arrangements
Additional Services	N/A
Location	<p>The Service under LOT 2 (PINS Service) shall be installed on OFFICIAL Cloud Hosting with AWS.</p> <p>Support services shall be performed primarily from the Supplier's offices in the UK.</p>
Quality Standards	n/a
Technical Standards:	<p>The technical standards used as a requirement for this Call-Off Contract are as per the service description on the G Cloud framework.</p> <p>The technical standards required for this Call-Off Contract are as set out in the Service Description Document, available here:</p> <p><u>PINS - Digital Marketplace</u></p> <p>https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/284971464066856</p>
Service level agreement:	<p>The service level and availability criteria required for this Call-Off Contract are as per the 'service definition document' on the G Cloud framework.</p>

	<p><u>PINS - Digital Marketplace</u></p> <p>https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/284971464066856</p>
Onboarding	<p>This contract provides for a continuation of an existing service, therefore onboarding activities are already complete.</p> <p>They included:</p> <ol style="list-style-type: none"> 1. Review technical requirements document provided by Saadian 2. Agree information sharing agreement with NOMS (PINS uses NOMS data) 3. Install by Saadian (Test and Production Environment) 4. User acceptance testing with business sponsor 5. On site user training delivered by Saadian <p>One of the key principles is that HMRC maintain ownership and control of HMRC data. The Supplier to make it easy to return the data to HMRC in a format that can easily be re-used.</p>
Offboarding	<p>The offboarding plan for this Call-Off Contract is,</p> <p>when off boarding, the handling of the data in PINS is governed by the information sharing agreement between the Buyer and HMPPS. The offboarding plan for this Call-Off Contract is:</p> <ul style="list-style-type: none"> • Buyer to notify Saadian in writing of your intention to exit. • Supplier to provide an export of HMRC specific data e.g. HMRC flags, HMRC offender lists and interests. But these will not be supported by the PINS database and data scheme. • Supplier to decommission the service and securely delete all data held, within 1 month of contract end.

Collaboration agreement	n/a
Limit on Parties' liability	<p>The annual total liability of either Party for all Property defaults will not exceed £1m.</p> <p>The annual total liability for Buyer Data defaults will not exceed £1m or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability for all other defaults will not exceed the greater of £ 1m or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>

Insurance	<p>The Supplier insurance(s) required will be:</p> <ul style="list-style-type: none"> • a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract. • Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law). • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Buyer's responsibilities	<p>The Buyer is responsible for</p> <ol style="list-style-type: none"> 1. The Buyer is responsible for agreeing access to prison data with NOMS. 2. The Buyer is responsible for controlling access to PINS data. 3. The Buyer is responsible for managing users access to PINS. 4. The Buyer is responsible for providing suitable training facilities for delivering training services.
Buyer's equipment	n/a

Supplier's information


Subcontractors or partners	Amazon Web Services (AWS) is the chosen partner for Saadian under this contract to provide Cloud Hosting for PINS.
-----------------------------------	--

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	<p>The payment method for this Call-Off Contract is Annual Purchase Order.</p> <p>Payment to be made via BACS or other electronic mechanism to our bank account.</p> <p>Bank Details</p> <p>██████████</p> <p>██████████</p> <p>██████████</p> <p>Payment for Software Services shall be made annually in advance.</p>
Payment profile	<p>The payment profile for this Call-Off Contract is upon completion of the following milestones:</p> <p>Year 1: Total Payable 1st April 2023 – £33,175 EX VAT Year 2: Total Payable 1st April 2024 – £33,175 EX VAT Year 3: Total Payable 1st April 2025 – £33,175 EX VAT</p> <p>At each anniversary of the contract hosting fees will be reviewed and amended in accordance with the AWS list price and any changes will be notified and agreed with the customer where applicable.</p> <p>Optional extension for HMRC: Year 4: Total Payable 1st April 2026 – £33,175 EX VAT</p> <p>The optional extension will be subject to price indexation in line with the Government's Office for National Statistics stated Retail Price Index figure at the time.</p>
Invoice details	<p>The Supplier will issue electronic invoices annually in advance via SAP Ariba. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.</p>

Who and where to send invoices to	<p>Invoices will be sent electronically via the SAP Ariba system to.</p> <p>██████████</p> <p>██████████</p> <p>Should hard copy invoices be required these will be sent to: Financial Shared Services Account Payable B Spur South Block Barrington Road Worthing West Sussex BN12 4XH</p>
Invoice information required	<p>All invoices must include purchase/limit order detail.</p>
Invoice frequency	<p>Invoice will be sent to the Buyer in advance of each annual renewal date as set out above.</p>
Call-Off Contract value	<p>The total value of this Call-Off Contract is £99,525 over (36 months) plus a 1 year extension option for an additional £33,175.</p> <p>Total = £132,700</p> <p>VAT to be applied to these figures.</p>
Call-Off Contract charges	<p>The breakdown of the Charges is HMRC is currently a PINS 5.1 Band A customer with an unlimited concurrent user Licence hosted by Saadian.</p> <p>HMRC is currently migrating to PINS 5.1 hosted by Saadian on the AWS cloud infrastructure and is scheduled to go live with the production service at which point the legacy PINS 4.4 service will be decommissioned.</p>

	<p>New functionality in PINS 5.1 includes the new analytical tools – stronger data visualisation enabling users to create link analysis highlighting significant connections and associations, enhanced search of data with and more flexible and personalised management of groups.</p> <p>The annual price for the PINS 5.1 Licence and Support is £18,025. The annual Cloud Hosting fee will be £15,150. This contract is offered under the terms of G-Cloud 13 and is available for an initial period of up to 36 months with an optional 12 months extension which we have included costs for below.</p> <p>The three year fee will be £99,525. As detailed in the quote attached following G-Cloud 13 pricing documents.</p> <p>HMRC Band A PINS 5.1 Licence & Support with Unlimited concurrent users, annual fee = £18,025.</p> <p>AWS Cloud hosting provider costs – tailored to meet Cloud hosting needs and preferences, annual fee = £6,300</p> <p>Saadian managed service fee for infrastructure and application support, annual fee £8,850.</p> <p>Total annual fee = £33,175</p> <p> HMRC PINS Renewal 2023_13.03.2023.pdf</p> <p>Optional PINS Training</p> <p>Professional Services</p> <p>PINS on line training session of 2.5 hours Training options include the standard generic PINS training for new or refresher users or this can be tailored around specific areas of the system to meet the needs of HMRC staff attending the session.</p> <p>On-site training can be offered and is subject to the SFIA rate card conditions below.</p> <p>Working Week – Monday to Friday excluding national holidays Office Hours - 09:00 – 17:00</p> <p>Monday to Friday Travel and Subsistence – Included in day rate within M25. Payable at department's standard T&S rates outside M25.</p>
--	---

	<p>Mileage – As above Professional Indemnity Insurance – included in day rate.</p> <p>Fee £600 per day.</p> <p>Terms and Conditions:</p> <ol style="list-style-type: none"> 1. G-Cloud 13 Terms & Conditions will apply. 2. All prices quoted exclude VAT <div data-bbox="564 607 616 667" data-label="Image"> </div> <p>284971464066856-s fia-rate-card-2022-01</p>
--	--

Additional Buyer terms

Performance of the Service	<p>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:</p> <ul style="list-style-type: none"> • Move to Version 5.1 – complete before 30th June 2023
Guarantee	n/a

Warranties, representations	As incorporated in the Framework Agreement clause 2.3.
Supplemental requirements in addition to the Call-Off terms	n/a
Alternative clauses	n/a
Buyer specific amendments to/refinements of the Call-Off Contract terms	<p>All data will be stored in Amazon Web Services Cloud hosting in the UK.</p> <p>Additional buyer terms. Supplemental requirements in addition to the Call-Off terms.</p> <p><i>The Supplier shall comply with the Authority's mandatory terms as set out in Schedule 9 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 9 will supersede any other terms in this Call-Off Contract.</i></p>

Personal Data and Data Subjects	<p>Annex 1 of Schedule 7 is being used:</p> <p>Personal data will be processed by Saadian.</p>
Intellectual Property	N/A
Social Value	<p>The 2 social values Sadiaan propose are:</p> <p>Fighting climate change</p> <p>Action includes, for example, efficiency of data centers, effectively managing server downtime when not required, reducing travel in particular international travel and using alternatives such as virtual meetings etc.</p> <p>Equal opportunity</p> <p>Action includes, for example, ensuring current equal opportunities policies and practices.</p>

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 clause 8.3 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 RM1557.13.

Signed	Saadian Technologies UK Ltd	The Commissioners for His Majesty's Revenue and Customs
Name	██████████	██████████
Title	██████████	██████████
Signature	██████████	██████████
Date	16/06/2023	16/06/2023

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

Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link:

[G-Cloud 13 Customer Benefit Record](#)

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 24 months.

2. Incorporation of terms

- 2.1 The following Framework Agreement clauses (including clauses 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)
 - 10 (Force majeure)
 - 5.3 (Continuing rights)
 - 5.4 to 5.6 (Change of control)
 - 5.7 (Fraud)
 - 5.8 (Notice of fraud)
 - 7 (Transparency and Audit)
 - 8.3 (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)
- 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 possible

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 14digit 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 invoices 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
- 9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:
- 9.8.1 premiums, which it will pay promptly
- 9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

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 trade marks 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 misappropriates 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 judgment 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-securityclassifications>

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: <https://www.cpni.gov.uk/content/adopt-risk-managementapproach> and Protection of Sensitive Information and Assets: <https://www.cpni.gov.uk/protection-sensitive-information-and-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/technology-code-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

19.6 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.

19.7 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 GDS 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 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

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 isn't 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

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.

29.3 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.

29.4 The Supplier will co-operate 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.

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

29.5.1 its failure to comply with the provisions of this clause

29.5.2 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

29.6 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.7 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 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. 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

The supplier is providing the PINS service to the buyer.

The Services, provided under LOT 2 (PINS Service), shall be installed in AWS Cloud assured hosting accessed by the customer from an approved network that has been given explicit permission to access the PINS web application.

Optional PINS Training

PINS on line training session of 2.5 hours Training options include the standard generic PINS training for new or refresher users or this can be tailored around specific areas of the system to meet the needs of HMRC staff attending the session.

On-site training can be offered and is subject to the SFIA rate card conditions below.

Working Week – Monday to Friday excluding national holidays Office Hours - 09:00 – 17:00

Monday to Friday Travel and Subsistence – Included in day rate within M25. Payable at department's standard T&S rates outside M25.

Mileage – As above Professional Indemnity Insurance – included in day rate.

Fee £600 per day.

Terms and Conditions:

1. G-Cloud 13 Terms & Conditions will apply.
2. All prices quoted exclude VAT



284971464066856-s
fia-rate-card-2022-01

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform 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:

This contract is offered under the terms of G-Cloud 13 and is available for an initial period of up to 36 months with an optional 12 months extension.

Total 3 year fee of **£99,525**. With an optional 12 months extension for **£33,175**.

Total **£132,700**

The three year fee will be £99,525. As detailed in the quote attached following G-Cloud 13 pricing documents.

HMRC Band A PINS 5.1 Licence & Support with Unlimited concurrent users, annual fee = **£18,025**.

The annual Cloud Hosting fee will be **£15,150**.

AWS Cloud hosting provider costs – tailored to meet Cloud hosting needs and preferences,
Annual fee = **£6,300**.

Saadian managed service fee for infrastructure and application support, annual fee **£8,850**.

Total annual fee = **£33,175**.

Schedule 3: Collaboration agreement - Not Applicable

Schedule 4: Alternative clauses - Not Applicable

Schedule 5: Guarantee - Not Applicable

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	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> 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 <p>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.</p>

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	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> • 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	<p>Default is any:</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
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 Information Commissioner 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.

Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • 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 <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • 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 <p>Majeure at the time this Call-Off Contract was entered into</p> <ul style="list-style-type: none"> • 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	<p>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).</p>
Framework Agreement	<p>The clauses of framework agreement RM1557.13 together with the Framework Schedules.</p>

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	<p>Can be:</p> <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium • a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • 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 • 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 • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>

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, judgment 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, judgment, 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.
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	<p>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:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ 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.
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-controlscheck-if-you-need-approval-to-spend-money-on-a-service
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-Off Contract) 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.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

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.

- 1.1 The contact details of the Buyer's Data Protection Officer are:
Data Protection Officer
advice.dpa@hmrc.gov.uk
- 1.2 The contact details of the Supplier's Data Protection Officer are:
Ed Wall Head of Operations
ewall@saadian.com
- 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 for each Category of Personal Data	<p>The Buyer is <u>Controller</u> and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the <u>Controller</u> and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> • The Custodial sentence terms, including the crime committed, number of sentences being served concurrently, custodial sentence start date, custodial sentence end date, and name and location of prison/institution where the custodial sentence was or is being served, for all custodial sentences for Individual Offenders who have served or are serving a custodial sentence • The Custodial sentence terms, including the crime committed, number of sentences being served concurrently, custodial sentence start date, custodial sentence end date, and name and location of prison/institution where the custodial sentence was or is being served, for all custodial sentences of individuals who are of interest to a police force or are wanted/missing.

	<ul style="list-style-type: none"> • Forenames, middle names, surnames, previous names, preferred pronouns, age, date of birth, gender identity, nationality, citizenship, status for right to remain in the United Kingdom, status for right to work in the United Kingdom, religion, occupation, current and previous names and locations of registered home addresses, names and locations of current and previous prison/ institution addresses, current and previous cell locations in prison/institutions where these custodial sentences were served or are being served, current and previous names and locations of places of employment, of Individual Offenders who have served or are serving a custodial sentence. • Forenames, middle names, surnames, previous names, preferred pronouns, age, date of birth, gender identity, nationality, citizenship, status for right to remain in the United Kingdom, status for right to work in the United Kingdom, religion, occupation, current and previous names and locations of registered home addresses, names and locations of current and previous prison/ institution addresses, current and previous cell locations in prison/institutions where these custodial sentences were served or are being served, and current and previous names and locations of places of employment, of individuals who are of interest to a police force or are wanted/missing.
--	---

	<p>The Supplier will not have direct physical access to any of the Buyer's Data from the Contract Start Date to the Contract End Date, or under any extension periods to this Call-Off Contract.</p> <p>The Supplier will have operational level access only to the data for the following processing activities to be carried out by the Supplier for the purposes of this contract:</p> <ul style="list-style-type: none"> • Installing and setting up a new Official Cloud Hosted PINS 5.1 service • Migrating the Buyer data from the current PINS 4.4 implementation to the new cloud hosted environment on Amazon Web Services (AWS). • Investigation and resolution of PINS service issues • Deployment of software and operational system patches <p>For any operational level access to the Buyers data for software defect resolution and/or deployment of patches the Supplier will do so in agreement with the Buyer and will operate through the change management process included as Appendix E and in compliance with the security controls outlined in the PINS cloud security principles (Appendix B) and PINS cloud service description (Appendix C).</p> <p>The only exception to this will be a service resolution for an immediate security risk to the operation or infrastructure which will be processed through an emergency change management process. The Supplier will inform the Buyer of these instances.</p>
--	--

	<p>PINS will be provided as an Official Hosted solution on AWS Cloud and all Buyer data will be stored within the AWS infrastructure and the location of all Buyer data will be stored in Europe – London (eu-west 2) region at all times.</p> <p>In addition to the HMPPS OFFLOC data, the Buyer (the Authority) may add their own local data (for which the Buyer is the Data Controller).</p>
--	--

Duration of the Processing	<i>The use of HMPPS's data by the Buyer (the Authority) in the PINS system will be used as required throughout the term of this Call-Off Contract.</i>
----------------------------	--

Nature and purposes of the Processing	<ul style="list-style-type: none"> • The Purpose of the Buyer using HMPPS's Data is to effectively manage Prisoners and their rehabilitation, and to provide support to other Law enforcement agencies using data provided by HMPPS. • The Supplier will not have direct physical access to any of the Buyer's Data from the Contract Start Date to the Contract End Date, or under any extension periods to this Call-Off Contract. • For the purposes of the contract the Supplier will have operational level access to migrate the Buyer Data from the existing PINS 4.4 to 5.1 by deploying the PINS 5.1 service to a new Cloud Official hosted server on AWS, supported by the Supplier and to support the operations for PINS for resolution and investigation of service issues and the deployment of software patching.
---------------------------------------	---

Type of Personal Data	<p><i>The Type of Personal Data under this Call-Off Contract will be:</i></p> <ul style="list-style-type: none"> • <i>The Custodial sentence terms, including the crime committed, number of sentences being served concurrently, custodial sentence start date, custodial sentence end date, and name and location of prison/institution where the custodial sentence was or is being served, for all custodial sentences for Individual Offenders who have served or are serving a custodial sentence</i> • <i>The Custodial sentence terms, including the crime committed, number of sentences being served concurrently, custodial sentence start date, custodial sentence end date, and name and location of prison/institution where the custodial sentence was or is being served, for all custodial sentences of individuals who are of interest to a police force or are wanted/missing.</i> • <i>Forenames, middle names, surnames, previous names, preferred pronouns, age, date of birth, gender identity, nationality, citizenship, status for right to remain in the United Kingdom, status for right to work in the United Kingdom, religion, occupation, current and previous names and locations of registered home addresses, names and locations of current and previous prison/ institution addresses, current and previous cell locations in prison/institutions where these custodial sentences were served or</i>
-----------------------	---

	<p>are being served, current and previous names and locations of places of employment, of Individual Offenders who have served or are serving a custodial sentence.</p> <ul style="list-style-type: none"> • Forenames, middle names, surnames, previous names, preferred pronouns, age, date of birth, gender identity, nationality, citizenship, status for right to remain in the United Kingdom, status for right to work in the United Kingdom, religion, occupation, current and previous names and locations of registered home addresses, names and locations of current and previous prison/ institution addresses, current and previous cell locations in prison/institutions where these custodial sentences were served or are being served, and current and previous names and locations of places of employment, of individuals who are of interest to a police force or are wanted/missing.
--	---

Categories of Data Subject	<p><i>This Data relates to:</i></p> <ul style="list-style-type: none"> • <i>Individual Offenders who have served or are serving a custodial sentence.</i>
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	<p><i>The Buyer (the Authority) will be the Controller of this Data. The Supplier will not have direct physical access to the Buyer's Data from the Contract Start Date to the Contract End Date, or under any extension periods to this Call-Off Contract.</i></p> <p><i>Data is retained on an ongoing basis to form a historic searchable data base for the Buyer (the Authority) and other UK police forces and appropriate national agencies.</i></p> <p><i>The local data added by the Buyer (the Authority) (for which the Buyer is the Data Controller) can only be searched and viewed by the Buyer.</i></p> <p><i>Upon termination of the contract, the Supplier will decommission the service and any HMPPS and HMRC provided data required to be retained by HMRC will be returned by the Supplier as part of the off boarding process referred to in Appendix C – PINS 5 cloud service description.</i></p>

Schedule 8: HMRC Travel & Subsistence Policy

HMRC Policy

HMRC Sustainable travel policy

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

How you can help deliver our business sustainably

You can help in two straightforward ways:

- Avoid travelling in the first place. This is about minimising your need to travel to meet your business objectives. You can change your working practices and help develop a culture which supports not travelling. For meetings your starting point should be that the meeting can be delivered effectively remotely. If you are responsible for setting up meetings you should take the lead on this. If meeting attendees, ask to use remote communication methods you should do all you can to achieve this. Travel for business can be essential in certain circumstances. Before you travel or ask others to travel on official business, you must decide whether your business objective can be achieved using alternatives. A well-run teleconference / Teams meeting can be as effective as a face-to-face meeting. It also saves 95% of the cost in expenses and staff time spent travelling.

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

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

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

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

Claiming expenses

- Claim only what you are entitled to claim in accordance with the T&S guidance below.
- Make sure you have receipts to support your claims as these are important in ensuring that HMRC achieves the same standards of record keeping as for its own staff and its contractors as HMRC expects of other taxpayers.
- Maintain your own personal record of expenses incurred as additional support to your claims
- Make sure you submit any claims within three months of the date the expenses are incurred, as this allows managers and budget holders to manage their resources more effectively.
- Only claim T&S for your meals and travel only, do not claim any element of T&S for your colleague's meal or travel as this may attract potential tax implication.
- A process for claims should be agreed with your contract manager at the start of the contract
- Your contract Manager will refuse to pay any claims above the stated rates
- Your contract manager can refuse to pay any claim where the Policy has not been met
- All HMRC T&S claims are subject to audit and public scrutiny

Journeys you can and can't claim for

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

Class of travel by Rail

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

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

Class of travel by Air

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

- The flight exceeds 2.5 hours
- No economy seats are available for flights of 2.5 hours or less.
- Exceptionally, you may travel first class if premium economy or business class seats are not available on a specific flight exceeding 2.5 hours that you need to catch.

Mileage allowances

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

Day Subsistence rates

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

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

Short-term Night Subsistence Allowances

Hotel Bed and Breakfast Capped Rates

At the following locations, actual expenditure incurred within these limits

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

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

Short-term Overnight Subsistence Allowances

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

Expenses for journeys you can't claim

If	then
your vehicle does not meet HMRC's insurance requirements; Business user is included	you can't claim mileage allowance.
expenses have been paid to you or are due to be paid to you by a third party - for example, another government department or organisation	you can't claim.
you incur parking penalties or fines for motoring offences	you can't claim.
you incur parking excess charges	you can't claim

Schedule 9: HMRC's Mandatory Terms

- A. For the avoidance of doubt, references to 'the Agreement' mean the attached Call-Off Contract between the Supplier and the Authority. References to 'the Authority' mean 'the Buyer' (the Commissioners for Her Majesty's Revenue and Customs).
- B. The Agreement incorporates the Authority's mandatory terms set out in this Schedule 9.
- C. In case of any ambiguity or conflict, the Authority's mandatory terms in this Schedule 9 will supersede any other terms in the Agreement.
- D. 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 are the definitions set out at Clause 1 of this Schedule 9.

1. 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"	<p>(a) the data, text, drawings, diagrams, <u>images</u> 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:</p> <p>(i) supplied to the Supplier by or on behalf of the Authority; and/or</p> <p>(ii) which the Supplier is required to generate, process, store or transmit pursuant to this Agreement; or</p> <p>(b) any Personal Data for which the Authority is the Controller, or any data derived from such Personal Data which has had any designatory data identifiers removed so that an individual cannot be identified;</p>
"Charges"	the charges for the Services as specified in the corresponding order form.
"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 <u>interpreted accordingly</u> ;
“Controller”, “Processor”, “Data Subject”,	take the meaning given in the UK GDPR;
“Data Protection Legislation”	(a) <u>“the data protection legislation”</u> as defined in section 3(9) of the Data Protection Act 2018; and; (b) all applicable Law about the processing of personal data and privacy;
“Key Subcontractor”	any Subcontractor: (a) 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 (b) 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:

	<ul style="list-style-type: none"> (a) the Supplier enters into a Subcontract; or (b) 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, <u>consultants</u> 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"	<ul style="list-style-type: none"> (a) all forms of tax whether direct or <u>indirect</u>; (b) national insurance contributions in the United Kingdom and similar contributions or obligations in any other <u>jurisdiction</u>; (c) all statutory, governmental, state, federal, provincial, local government or municipal charges, duties, imports, contributions, levies or liabilities (other than in return for goods or services supplied or performed or to be performed) and withholdings; and (d) any penalty, fine, surcharge, interest, <u>charges</u> or costs relating to any of the above, <p>in each case wherever chargeable and whether of the United Kingdom and any other jurisdiction;</p>
"Tax Non-Compliance"	<p>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:</p> <ul style="list-style-type: none"> (a) the "Economic Operator" means the <u>Supplier</u> or any agent, supplier or Subcontractor of the Supplier requested to be replaced pursuant to Clause 4.3; and (b) 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.

2. Payment and Recovery of Sums Due

2.1 The Supplier shall invoice the Authority as specified in Clause 7 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:

2.1.1 the Supplier does so at its own risk; and

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

2.2 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.

2.3 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.

3. Warranties

3.1 The Supplier represents and warrants that:

3.1.1 in the three years prior to the contract start 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;

3.1.2 it has notified the Authority in writing of any Tax Non-Compliance it is involved in; and

3.1.3 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 contract start date.

3.2 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.

3.3 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).

4. Promoting Tax Compliance

- 4.1** 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.
- 4.2** 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.
- 4.3** 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.
- 4.4** If, at any point during the Term, there is Tax Non-Compliance, the Supplier shall:
- 4.4.1** notify the Authority in writing of such fact within five (5) Working Days of its occurrence; and
- 4.4.2** promptly provide to the Authority:
- (a)** 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
 - (b)** such other information in relation to the Tax Non-Compliance as the Authority may reasonably require.
- 4.5** 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.
- 4.6** 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.

4.7 If the Supplier:

- 4.7.1** 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 may be a material breach of the Agreement;
- 4.7.2** 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
- 4.7.3** 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).

- 4.8** 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.

5. Use of Off-shore Tax Structures

- 5.1** 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.

- 5.2** 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.
- 5.3** 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.
- 5.4** 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).

6 Data Protection and off-shoring

- 6.1** 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:

6.1.1 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:

- (a)** 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;
- (b)** the Data Subject has enforceable rights and effective legal remedies;
- (c)** 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
- (d)** 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;

- 6.2** 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).

7 Commissioners for Revenue and Customs Act 2005 and related Legislation

- 7.1** 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.
- 7.2** 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.
- 7.3** 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 the Official Secrets Acts 1911 to 1989 and the obligations set out in Section 182 of the Finance Act 1989.
- 7.4** 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.
- 7.5** 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.
- 7.6** 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).

8. Confidentiality, Transparency and Publicity

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

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

8.1.2 use the Authority's name or brand in any promotion or marketing or announcement of orders, except with the prior written consent of the Authority.

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

8.3 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Agreement is not Confidential Information. The Authority shall be responsible for determining in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the

provisions of the FOIA. Notwithstanding any other term of this Agreement, the Supplier hereby gives his consent for the Authority to publish the Agreement in its entirety, (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted) including from time to time agreed changes to the Agreement, to the general public. The Authority may consult with the Supplier to inform its decision regarding any redactions but the Authority shall have the final decision at its absolute discretion.

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

9. Security Requirements

The Supplier shall comply with the security management plan set out in the call off contract 'Completed Security Plan Questionnaire', ("Security Management Plan") and the security policy identified as such within the Security Management Plan ("Security Policy").

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

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 which is either: ("X")
 - 1) The Economic Operator or Essential Subcontractor (EOS)
 - 2) Part of the same Group of companies of 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*¹;
 - 3) 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)

2. X has been engaged in one or more of the following:
 - a. Fraudulent evasion²;
 - b. Conduct caught by the General Anti-Abuse Rule³;
 - c. Conduct caught by the Halifax Abuse principle⁴;
 - d. Entered into arrangements caught by a DOTAS or VADR scheme⁵;
 - e. Conduct caught by a recognised 'anti-avoidance rule'⁶ 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 affected 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;
 - f. Entered into an avoidance scheme identified by HMRC's published Spotlights list⁷;
 - g. 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))

3. X's activity in *Condition 2* is, where applicable, subject to dispute and/or litigation as follows:
1. In respect of (a), either X:
 1. Has accepted the terms of an offer made under a Contractual Disclosure Facility (CDF) pursuant to the Code of Practice 9 (COP9) procedure⁸; or,
 2. Has been charged with an offence of fraudulent evasion.
 2. In respect of (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.
 3. In respect of (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.
 4. In respect of (f) this condition is satisfied without any further steps being taken.
 5. In respect of (g) the foreign equivalent to each of the corresponding steps set out above in (i) to (iii).

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: SR1317244952, 1st April 2023 ('the Agreement')

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.


SIGNED:
FULL NAME: Jennie Jablonski
POSITION: Head of Sales
COMPANY: Saadian Technologies UK Ltd
DATE OF SIGNATURE: 26 th April 2023

Completed Security Plan Questionnaire.



Security Plan Questionnaire - Medium

To:	Saadian Technologies UK Ltd
From:	Kane Davies, HMRC Commercial Directorate.
Date:	17.03.2023
Tender reference:	11800 & PINS Licenses and Support. RM1557.13-All- H M Revenue & Customs
Tender title:	Saadian PINS - RM1557.13

Schedule 2.4 Security Plan

Background
<p>PINS is a Prisoner Intelligence Notification System that enables justice and law enforcement agencies to keep track of offenders when they are in prison and when they are released from prison.</p> <p>Since its introduction in 2003, PINS has been developed based on feedback from our law enforcement customers. Sending over one million prison release notifications each year, PINS acts as an essential early warning system, helping criminal justice agencies prevent re-offending. PINS helps over 47 UK local and national law enforcement agencies prevent re-offending by proactively notifying local criminal justice officers of prison releases into their local area 4 weeks in advance.</p> <p>Over the years, PINS has developed into a critical intelligence tool, integrating prison data with prolific offender data, outstanding warrants, organised crime groups and electronic monitoring data. The current supported versions of PINS are v4.4 and v5.1 which is our latest digital platform designed with significant enhancements.</p> <p>The PINS service in HMRC provides prison data from NOMIS and enables HMRC to upload its own data and automatically cross references and links historic and current prisoner records. Daily monitoring of prison data allows PINS to send critical alerts and notifications to intelligence officers detailing key prisoner data changes as well as advance release notifications</p> <p>Features of PINS include:</p> <ul style="list-style-type: none"> • Single view of an offender across multiple periods of custody • Add watches to prisoners for notifications of changes (including cell changes) or release • Search prison inmates by crime, nationality and prison location • Import and match current PPO/IOM lists from IDIOM or Excel • Track gang and organised crime nominals • Automatically match outstanding warrants • Bulk check any Excel list of offenders against prison inmates • Show clear visibility of historic and current cell and wing sharing arrangements
1 Policy & Standards
<p>1a Please confirm that you understand that your responses to this questionnaire will form the initial Security Plan and will be included in the final signed version of any resulting agreement.</p> <p>Yes</p>
<p>1b Please confirm your organisation and any subcontractors' will conform to the requirements set out in the Government Security Policy Framework (SPF), available from Security Policy Framework and any Security Requirements recorded in the schedules and/or Order Form.</p> <p>Yes</p>

<p>1c If you believe that the Public Sector Network (PSN) Code of Connection, available from www.gov.uk, will apply to your organisation and any sub-contractors, please provide details of how you will conform to this.</p>
Not applicable
<p>1d Please confirm that your organisation and any sub-contractors will handle HMRC assets in accordance with legislation including the UK General Data Protection Regulation see UK GDPR and in accordance with Call-Off Schedule 23 (HMRC Terms) and clause 14 (Protection of Data) of the CCS Core Terms of the Contract.</p>
<p>Saadian has performed a review of their service provisions and data handling (both for clients and staff) to ensure adherence to GDPR, which is reviewed annually. We created and published or circulated where appropriate, privacy, data protection, data retention, information security and SYOPS policies for each service. Where remediation was required within our services to meet these new policies, changes were implemented to manage data retention and to support right to be forgotten requests.</p>
<p>1e Please confirm that you have paid the Data Protection Fee to the ICO or that you fall into one of the exempt categories. More information can be found here</p>
Saadian are exempt as we don't determine how personal data is processed
<p>1f Please provide details of any security accreditation that your organisation currently possess, such as but not exclusive to, ISO27001 and PCI DSS and describe the process used to achieve the accreditation.</p>
<p>Saadian holds Cyber Essentials certification and is working towards certifying ISO 27001.</p> <p>Amazon Web Services (AWS) is Saadian's partner for Cloud Hosting of PINS for HMRC and is a STAR certified cloud provider and both implement and are certified to ISO27001 and Cyber Essentials Plus.</p>
<p>1h As appended to this Schedule 2.4, Appendix G, Security Aspects Record, defines the Government Security Classifications (see Government Security Classifications) carried by the HMRC data. If you are successful in the tender process, you will require a Security Manager (or appointed person), to take responsibility for the security of the data.</p> <p>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).</p>
<p>Ed Wall Head of Technical Operations ewall@saadian.com</p>

<p>2 Physical Security (For requirements please see Appendix A – Physical Security)</p>
<p>2a For the locations where HMRC assets are held please provide details of any procedures and security in place designed to control access to the site perimeter.</p> <p>Detail measures such as fencing, CCTV, guarding, and procedures and controls in place to handle staff and visitors requesting access to the site.</p> <p>Please also provide details of the maintenance schedule of your security controls.</p>
<p>No data or processing is stored or provided directly from Saadian premises.</p> <p>Saadian use AWS for infrastructure services, data storage and processing. Their physical premises and UK (London) datacentres and services have been PASF assessed and are secured to a level satisfying the Home Office and National Policing Information Risk Management Team. (https://aws.amazon.com/blogs/security/aws-eu-london-region-selected-to-provide-services-to-support-uk-law-enforcement-customers/)</p> <p>AWS List of Security Controls is available here: https://aws.amazon.com/compliance/data-center/controls/</p>
<p>2b Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas holding HMRC assets.</p> <p>Detail measures such as construction of buildings used for handling HMRC assets, 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.</p> <p>Please also provide details of the maintenance schedule of these security controls.</p>
<p>No data or processing is stored or provided directly from Saadian premises.</p> <p>Saadian use AWS for infrastructure services, data storage and processing. Their physical premises and UK (London) datacentres and services have been PASF assessed and are secured to a level satisfying the Home Office and National Policing Information Risk Management Team. (https://aws.amazon.com/blogs/security/aws-eu-london-region-selected-to-provide-services-to-support-uk-law-enforcement-customers/)</p> <p>AWS List of Security Controls is available here: https://aws.amazon.com/compliance/data-center/controls/</p>

<p>3 IT Security (For requirements please see Appendix B – IT Security) Please state what, if any, form of assessment in relation to the Government backed Cyber Essentials Scheme has been performed. If no assessment has been performed please answer all questions in this section.</p> <p>3a Please state what, if any, form of assessment in relation to the Government backed Cyber Essentials Scheme has been performed. If no assessment has been performed please state when you expect it to be completed.</p> <p>Saadian maintain annual certification for CyberEssentials.</p> <p>AWS, from where the services are provided and the data stored, hold and maintain CyberEssentials Plus: https://aws.amazon.com/compliance/cyber-essentials-plus/</p> <p>3b Please provide details of the controls and processes you have in place covering patching, malware (anti-virus), boundary/network security (intruder detection), content checking/blocking (filters), lockdown (prevention) and how regularly you update them.</p> <p>Saadian use industry standard antivirus on operating systems with interactive access, including engineer desktops and within the secure network perimeter and web application firewalls where necessary on published service endpoints.</p> <p>All employee devices are centrally managed and adhere to a strict patching schedule and provide support for secure remote-erasure of data. Servers are patched at least quarterly through our change management process, or more frequently where critical security patches are identified.</p> <p>3c Please provide details of the overall security and access control policy of your systems covering physical and electronic assets (including communications connection equipment, e.g. bridge, routers, patch panels). You should record details of the formal registration/deregistration process, how users are Authorised, Authenticated and held Accountable for their actions. Also include details of the measures in place to manage privilege access e.g. System Administrators and remote users.</p> <p>Saadian implement ISO27001 standards, including reporting frameworks for information security events and security weaknesses; the output of which create work items as part of our continuous improvement processes. This includes the auditing and management of user access controls. Saadian doesn't maintain any production physical IT assets and so the physical controls are managed by Amazon Web Services, again, through ISO27001 and additional security standards (further details available from AWS).</p> <p>3d Please provide details of how your security and access control policy complies with the Security Policy Framework including where necessary, use and control of back up systems, network storage and segregation of HMRC data (including 'cloud' solutions), and additional security for more sensitive information assets.</p>
<p>Saadian staff are provided limited time access to sensitive production data or services to implement approved changes or diagnostics. Beyond anonymous telemetry data and remote recovery procedures. Each data access request is reviewed and approved as part of the change management process.</p> <p>Sensitive data classified at UK OFFICIAL is restricted to dedicated network and infrastructure environments, with each customer contained within their own segregated network. All Saadian team members with access to customer and UK OFFICIAL data are cleared to NATIONAL NPPV3 WITH SC and UK based.</p> <p>3e Please describe how you ensure all software and data is approved before being installed, and how your information systems are reviewed for compliance with security implementation standards (e.g. penetration testing).</p> <p>Security and device configuration is defined in our ISMS; Saadian employee devices are provisioned and managed centrally and provide secure, remote wipe or retire facility.</p> <p>We also have an audit policy to check the software which is required and not required for each employee. The Admin group review these on a monthly basis and remove them from the user system manually.</p> <p>3f Please provide details of the controls and processes (including level of encryption and controlled access procedures) you have in place for the use of portable media and storage devices exceptionally loaded with HMRC data.</p> <p>HMRC data is never transferred on to portable media, all data is encrypted at rest within the network perimeter to AES-256. Data egress is possible only by client request through time-limited, IP restricted access to SFTP or similar transfer methods exceeding those standards.</p> <p>3g Please provide details of how all equipment (e.g. hardware, portable media) that holds or has held data will be destroyed or decommissioned and how all data will be rendered unreadable and irretrievable in line with the Security Policy Framework.</p> <p>All data is held on virtual infrastructure in our cloud service providers. Data held on virtual disks (EBS volumes) attached to servers is securely deleted immediately upon termination and the encryption keys are destroyed with the key management system. AWS follow the sanitisation process outlined in this document, published by NIST: https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final</p> <p>If additional measures are required, we can perform a secure delete and block level overwrite on the encrypted volumes per NCSC guidance for physical disks https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media</p>

4 Personnel Security (For requirements please see Appendix C – Personnel Security)
4a Have all staff who will have access to, or come in to contact with HMRC data or assets undergone Baseline Personnel Security Standard checks (See www.gov.uk for further information).
All staff who have access to HMRC information are vetted through the National Contractor Vetting Scheme NATIONAL NPPV 3 WITH SC Our vetting is carried out by: Warwickshire Police Vetting Unit, Stratford upon Avon Police Station, Rother Street, Stratford Upon Avon, CV37 6RD
4b Please provide details of how you will ensure that all staff accessing HMRC data are aware of the confidential nature of the data and comply with their legal and specific obligations under the Contract?
All Saadian employee contracts include a confidentiality clause and are required to undertake annual security training and how that relates to the handling of sensitive data that their NPPV3 & SC clearance permits.
4c All contractor's personnel who have access to HMRC data, and/or are directly involved in the service provision must sign a copy of HMRC's Confidentiality Agreement. Please confirm that, in the event that your bid is successful, you will provide signed hard copies of the CA for all personnel involved in this Contract if requested.
Yes
5 Process Security (For requirements please see Appendix D – Process Security)
5a Please provide details of the format in which HMRC data will be held, how you will ensure segregation of HMRC data, and the locations where this data will be processed.
All HMRC Data is stored, and services provided from, AWS London (UK) Data Centres. Support is provided only from within the UK, by NPPV3/SC cleared, UK based engineers. Supplementary technical assistance may additionally be provided by engineers in Dublin, Ireland under direct supervision by and in close collaboration with UK based, NPPV3/SC cleared personnel. HMRC data is separated from other tenants at an "Account" level within AWS, following their recommendations. This provides complete separation of production data from other customers and systems. Data is primarily stored in encrypted MSSQL or MySQL database clusters, on encrypted EBS volumes. Prison data ingested data from HMPPS is retrieved directly from the OFFLOC endpoint and stored initially on encrypted EBS volumes before local processing into the system. The OFFLOC files themselves are then individually encrypted and stored on a secured S3 volume within the same AWS Account for the purposes of resilience and recovery, for the HMRC service only.
5b Please confirm your understanding and agreement that the transfer of any HMRC asset to third parties (any individual or group other than the main Contractor) is prohibited without prior written consent from HMRC. If you anticipate transferring data, especially using portable media during the delivery of this project, please set out your proposed transfer procedures for consideration.
Saadian will not transfer or otherwise share any HMRC data to any third parties.
5c – Part 1 Please confirm that you understand that 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.
Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>
5c – Part 2
If you are considering offshoring HMRC data, please provide details on where and how you will ensure it is secure.
Will you be offshoring Personal Data shared by HMRC? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
1. Will you be offshoring the Personal Data shared by HMRC to a non-adequate country? (A list of countries covered by adequacy regulations can be found here) Yes <input type="checkbox"/> No <input type="checkbox"/> Please state the country/countries here _____
To the extent that any data offshoring would include offshoring to any non-adequate country, 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.
Please note: In line with HMRC's current policies, the successful supplier(s) will not be permitted to offshore any Personal Data provided by HMRC in connection with any contract resulting from this procurement exercise to any non-adequate country where such offshored data will not be subject to an appropriate safeguard and will not be afforded a level of protection essentially equivalent to that guaranteed in the UK by UK GDPR.
On this basis, HMRC reserves the right to reject a bidder's entire tender submission and/or terminate any contract awarded where it becomes apparent to HMRC that the supplier is offshoring/is proposing to offshore Personal Data to a non-adequate country both without an appropriate safeguard and without ensuring the transferred data is afforded a level of protection essentially equivalent to that guaranteed in the UK by UK GDPR. If requested by HMRC, a Transfer Risk Assessment (Appendix H) will need to be completed if you are considering offshoring personal data to a country that is not covered by an adequacy decision.

5d In order to protect against loss, destruction, damage, alteration or disclosure of HMRC data and to ensure it is not stored, copied or generated except as necessary and authorised, please provide details of the technical and organisational measures you have in place (including segregation of duties and areas of responsibility) to protect against accident or malicious intent.
Access to HMRC data and services is closely controlled, monitored and audited. There are alarms in place for any attempts to modify the data, security or network configuration from Saadian's implementation of the AWS and NCSC security recommendations; these recommendations prevent egress or transfer of data from the production environment. The SC cleared service engineers with access to HMRC data do not have permission or responsibility for managing cloud security or network configuration, which are governed at an by the technical leadership at an organisational level.
5e What arrangements are in place for secure disposal of HMRC assets once no longer required?
Saadian have a decommissioning procedure for cloud hosted assets, which includes the individual termination and validation of all storage media and the termination and closure of the AWS account providing the services, without any data leaving its perimeter.
5f How will you immediately advise HMRC of security incidents that impact HMRC assets?
Security incidents are reported to affected customers or partners where relevant, regular, holistic or specific review and reporting frequency is determined by mutual agreement with the client and the terms of the SLA. Saadian implement ISO27001 standards, including reporting frameworks for information security events and security weaknesses; the output of which create work items as part of our continuous improvement processes.

6 Business Continuity (For requirements please see Appendix E – Business Continuity)

6a Please provide an overview of your organisation's business continuity and disaster recovery plans in terms of the HMRC data under the Contract, or attach a copy of your Business Continuity Plan.

HMRC data within the PINS Cloud service is backed up to multiple physically discrete "availability zones" ([an AZ is one or more discrete data centres](#)) within the UK AWS regions.

In the case of HMRC data and services requiring recovery through system or data failure, Saadian will attempt to recover to a system backup within the last 48 hours (RPO) and to complete the recovery process within 72 hours (RTO). The (HMRC) PINS Cloud system can be re-deployed from our software and configuration repositories, which are highly available and multi-region.

If required, contractual recovery SLAs (RPO, RTO), Off-Site/Multi-Site recovery options can be included in addition to the service availability SLA. If necessary for customer operational resilience, further "Off Site" backups and recovery to an agreed alternate cloud location or to HMRC locations can be agreed additionally.

7 Cryptography

7a Will you be using commercial cryptography as part of this contract? If so, please provide details.

Saadian follow the [NCSC cloud security principles](#) and [guidelines](#) on the use of commercial cryptographic software and hardware solutions. PINS Cloud solutions use AWS Secret Manager (<https://docs.aws.amazon.com/secretsmanager/latest/userguide/secretsmanager-compliance.html>) and AWS Key Management Service (<https://docs.aws.amazon.com/kms/latest/developerguide/kms-compliance.html>). AWS Secrets Manager uses envelope encryption with AWS KMS keys, stored on FIPS 140-2 HSMs <https://docs.aws.amazon.com/kms/latest/developerguide/data-protection.html>

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, and must 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 should be identifiable and escorted at all times	Visitors to be issued with identifying badges upon arrival. A visitor log maintained and visitors sign-in and out.
Building	Should be constructed of robust building materials typically, brick or lightweight block walls. External doors should be of solid construction and locked during silent hours. Access to keys should be checked and any lock combinations changed at regular intervals not exceeding 12 months. A record of key/combination holders should be maintained. The number of keys to a lock should be kept to a minimum. Spare keys should 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 should 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 processes agreed with HMRC.	Point to point transport of material in locked containers.

Appendix B – IT Security

IT Security	Requirements	Recommended
Cyber Essentials	It is a requirement for HMG suppliers to have undertaken self-assessment and achieved the Government backed Cyber Essentials scheme.	Cyber Essentials Plus with independent assessment and certification.
Authorisation	Users and Administrators must be authorised to use the System/Service.	
Authentication ¹	Individual passwords must be used to maintain accountability; Robust passwords should be used that are designed to resist machine based attacks as well as more basic guessing attacks. Passwords must be stored in an encrypted form using a one-way hashing algorithm. Passwords must be able to be changed by the end user, if there is suspicion of compromise. Passwords must be changed at least every 3 months.	Machine generated passwords. Multi-factor authentication should be considered for exposed environments and remote access. Passwords for privileged accounts/users (Administrators) etc. should be changed more frequently than every 3 months.
Access Control	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	Controls such as anti-virus software must detect and prevent infection by known malicious code. ³ AV Administrators and users should be trained on use of AV software. Users should receive awareness training so that they are aware of the risks posed by malicious code from the use of email and	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.

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).

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.

³ Heuristic scanning capabilities can help detect against previously undocumented attacks but AV products are generally ineffective against day zero attacks and are therefore only effective against known malicious code attacks. It is important therefore that systems and applications are locked down, patched against known vulnerabilities that could allow execution of malicious code e.g. in browsers and email clients.

	<p>attachments, internet and removable media (CD, DVD, USB devices etc).</p> <p>Software should be patched and devices, systems, operating systems and applications should be 'locked down' to remove unnecessary services and functionality.</p> <p>File types should be limited.</p> <p>System designs/architectural blue prints and network designs should be protected from unauthorised access, loss and destruction.</p> <p>All users, systems and services must be provided on a least privilege basis to reduce the potential for accidental introduction of malicious code.</p> <p>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 attacker.</p> <p>For systems attaching to HMRC network, dual layered malware protection and detection capability.</p>	
Network Security	Boundary controls that have a content checking and blocking policy in place e.g. firewalls.	<p>Dual paired firewalls, different vendors.</p> <p>Anomaly detection capability e.g. Network intruder detection system.</p>
Patch Management	<p>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.</p> <p>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.</p>	
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.	<p>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.</p> <p>Approval from HMRC must be obtained before information assets are placed on removable media⁴. This approval must be documented sufficiently to establish an audit trail of responsibility.</p> <p>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.</p>	

Appendix C – Personnel Security

Personnel Security	Requirements	Recommended
Pre-employment checks	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 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.

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

Appendix D – Process Security

Process Security	Requirements	Recommended
Security Policies, Processes and Procedures	<p>Procedures to be in place to determine whether any compromise of HMRC assets e.g. loss or modification of information, software and hardware has occurred.</p> <p>Procedures for the handling and storage of HMRC information assets should be established to protect from unauthorised disclosure and/or misuse.</p> <p>End of day procedures should ensure that HMRC assets are adequately protected from unauthorised access.</p> <p>A clear desk policy should be enforced.</p> <p>Procedures must be in place to ensure the HMRC's assets are segregated from any other Client's assets held by the contractor.</p> <p>Procedures for the secure disposal of the HMRC's assets must be in place.</p> <p>A challenge culture should be fostered, so that unknown staff or visitors are challenged. Where an access control system is used tailgating should be discouraged.</p>	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	<p>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.</p> <p>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.</p>	<p>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.</p> <p>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.</p>
Incident Management	Arrangements should be in place for reporting security breaches to the asset owner.	

Business Continuity Requirements	Requirements	Recommended
Business Continuity Management	3 rd 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	

	Requirements	Recommended
Commercial Cryptography	Where you intend to use commercial cryptography as a layer of security for HMRC data at rest or during processing please provide details of the product you intend using and confirmation of appropriate licencing.	

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:-

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.

Appendix H - Transfer Risk Assessment

NOTE: These questions **DO NOT** need to be completed unless specifically requested by HMRC, in the event offshoring of personal data in a non-adequacy country has been identified (Question 5c).

Step 1: Assess the transfer

1. What is the name of the supplier/organisation?
2. What type of entity is the organisation?
3. What is the role of the organisation?
4. How often will these transfers occur?
5. What is the volume of personal data being transferred?
6. What types of personal data are being transferred?
7. In what format will the personal data be transferred? i.e encrypted, plain text, pseudonymised, password protected
8. Do you consider that your organisation has the appropriate level of technical and organisational measures to process personal data securely?
9. Will there be a requirement for the personal data to be forwarded on by the supplier to another entity?
10. Have retention periods been set and documented? (storage limitation principle)

Step 2: Destination Country Assessment

Legal Regime Assessment

1. Name of destination country
2. Does the organisation have a Privacy Notice in place for this processing?
3. Does the country have an established legal system in place?
4. Will a foreign judgement or arbitration be recognised (acknowledged) and enforced in the destination country? i.e. If a judgement or arbitration was made in the UK would the destination country uphold this?
5. Is the jurisdiction party to one of the following conventions for recognition of enforcement of foreign judgments or arbitration awards?
 - o the Brussels Convention; or
 - o the Hague Choice of Court Convention

Note: If the destination has signed up to one of these conventions – it is accepted that they would recognise and enforce foreign judgements or arbitration
6. Is there independent judiciary where individuals can seek access to justice and means for redress?
7. Are the rights of the data subjects under the third-party beneficiary clause in contracts recognised and enforced in the destination country?
8. Does the destination country have high levels of integrity and independence in the judicial process? i.e. - Is there any corruption in the legal system? Is there a division of power? (for example, in the UK we have a separate judiciary in the police force, i.e., if an individual wanted to seek justice against the police the court system acts independently from the police they do not work as one body.
9. Does the destination country have mature data protection and/or privacy laws in place?

Surveillance Assessment

1. Do public authorities have wide powers to intercept communications and to access data from private companies, with few, if any safeguards?

2. Do law enforcement agencies and other public authorities request information from private sector companies? If so, what would be the reason for these requests? Are requests deemed excessive and at a disproportionate level? How many requests has your company received to date, from law enforcement agencies which may include data about individuals?
3. Are there rules for setting out when private companies are able to obtain access to data? For example, by Court Order?
4. Would it be reasonable to believe that the data subjects and/or the categories of personal data would be of interest to third parties and/or public authorities?
5. Please provide us with a link to the relevant legislation that governs the interception and third-party access of data. i.e. What piece of legislation enables the disclosure of personal data to law enforcement agencies and other public authorities? What piece of legislation restricts the disclosure of personal data to law enforcement agencies and other public authorities?
6. Is HMRC employee data e.g. IP addresses collected as part of this processing activity?
 - a. If so, will you be undertaking workplace monitoring on any or all HMRC employees/contractors/agency workers? If yes, please forward a copy of your policy document
 - b. Is this processing authorised under the supplier contract/agreement?
 - c. What safeguards will be in place?